Ciberseguridad: Resumen de Amenazas 2021 y Tendencias 2022

"There's no silver bullet solution with cyber security, a layered defense is the only viable defense"

James Scott

ÍNDICE

ÍNDICE

ÍNDICE

INTRODUCCIÓN

2021, un año que hemos definido como el año del equilibrio. Acuñamos este término debido a diversos hechos que marcaron un quiebre frente a la entropía que se vivió durante finales de 2019 y 2020 por una crisis global sin precedentes.

Durante este año, vimos cómo la crisis sanitaria fue siendo emancipada gracias a la implementación de protocolos y aparición de vacunas, cuyos frutos conllevaron a que distintas empresas de todas las industrias lograran normalizar sus operaciones con un retorno laboral híbrido de sus colaboradores (presencial y no presencial).

Del mismo modo, en el ambito de ciberseguridad, pese a que fue un año marcado por nuevas amenazas con revuelo mundial, es importante destacar un hito que extrañamente tuvo poco impacto mediático: **2021 fue el año donde se registró el mayor número de operaciones conjuntas y combinadas contra actores de amenazas y portales de mercado negro.** Este hecho ha generado un ambiente disuasivo que llegó para instaurar un escenario esperanzador, definiendo que los cibercriminales ya no tienen libre albedrío y son objetivo de instituciones gubernamentales que están actuando de forma organizada para sofocar la vertiginosa alza del cibercrimen.

El equilibrio también se visualiza en **la normalización y adopción de los avances en digitalización** que han conllevado las organizaciones muchas veces sin una carta de navegación definida.

Es un hecho, que durante el último decenio la conectividad a internet ha aumentado de forma exponencial y se ha instaurado como parte intrínseca de nuestros quehaceres. La humanidad ha generado hábitos arraigados a la dependencia tecnológica los cuales, en gran medida, son beneficiosos para la productividad cotidiana, otorgando simplicidad y eficiencia en nuestra rutina.

No obstante, en 2020, la pandemia impuso un desafío para todas las industrias del mundo: **mantenerse en el mercado.** De esta forma, las organizaciones más innovadoras adoptaron el cambio de paradigma y gracias a la transformación digital lograron alcanzar un modelo de madurez sustentable para mantener sus operaciones de negocio a la vanguardia, destacando por sobre las demás.

"La participación del ecommerce en el mercado nacional, era sólo de 7% antes de la pandemia. En 2021 las ventas en retail llegaron al 30,5% del total."

Cámara Nacional de Comercio (CNC)

Bajo el mismo contexto, producto del escenario ocasionado por la pandemia, aquellas organizaciones inmaduras y escépticas fueron obligadas a transformarse digitalmente, forzando la implementación de recursos, cultura, procesos y herramientas tecnológicas en tiempos récord. En otras palabras, la transformación digital fue instaurada globalmente como una vía de subsistencia, convirtiéndose en la principal herramienta para continuar y fortalecer las operaciones de negocio las empresas.

A medida que la pandemia continuó perturbando los sistemas mundiales, hubo otra amenaza poco visible que fue en aumento en el espacio digital: el cibercrimen y las ciberoperaciones delictivas perpetradas por actores maliciosos con grandes destrezas, quienes tienen financiamiento suficiente como para soportar campañas de largo aliento y con las habilidades necesarias para cumplir sus objetivos.

Lo cierto, es que esto es sólo un breve resumen de hechos conocidos, que ocurrieron durante 2021 y que continuarán en 2022 si no cambiamos la forma de enfrentar estos riesgos.

CONTEXTO

¿Por dónde debemos fortalecer el resguardo de nuestros sistemas y proteger nuestros datos?

Gran parte de la explotación de vulnerabilidades evidenciada a la fecha, **se ha gestado por una falta de mitigación oportuna.** En efecto, a nivel nacional, hemos logrado colectar estadísticas que han demostrado un escenario desfavorable para Chile.

Menos del 16% de las vulnerabilidades se corrigen dentro de los 7 días posteriores a la notificación por parte de las marcas.

Empresas con políticas maduras para parchear infraestructura

<41%

Vulnerabilidades que se corrigen luego de

7 días

<16%

Menos del 41% de las empresas tienen políticas maduras para el parcheado de su infraestructura, esto quiere decir que más de la mitad de las organizaciones no están aplicando las actualizaciones necesarias de sistemas y plataformas en sus infraestructuras, **lo que deja un importante campo abierto sin protección, favoreciendo a que ciber actores maliciosos** logren explotar estas vulnerabilidades con las consecuencias ya advertidas.

A estas brechas, se añaden lo particular de estos dos últimos años tensionados por la pandemia, empresas principiando en la modalidad de tele-trabajo y a la disminución de personal en algunos equipos: un escenario perfecto para atacar a los más desprevenidos.

Si bien es natural que la dirección de las organizaciones privilegie la operación por sobre la seguridad; la madurez de sus operaciones siempre estará ligada a infraestructura digital, es por ello que las gerencias deben tener visibilidad y entender el impacto que involucra para el negocio la exposición de sus datos e infraestructura por falta de actualización oportuna, es decir por la ausencia de políticas maduras de parcheado.

¿Cuál es el desafio para las organizaciones ?

El reto de las organizaciones está en entender la criticidad del problema, en contar con tecnologías adecuadas que prevengan este tipo de amenazas junto con la concientización de sus colaboradores, quienes siguen siendo el eslabón más débil y principales responsables de la entrada de ciberataques.

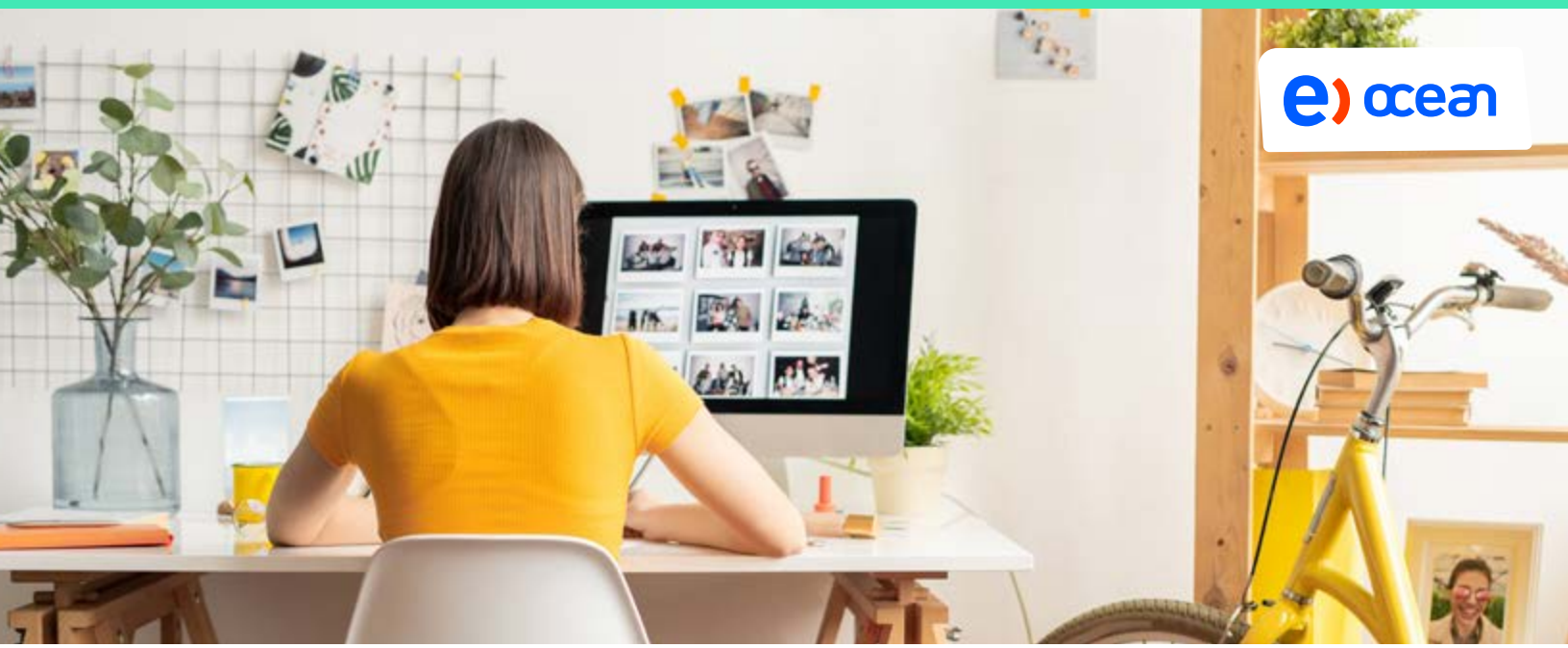
Como Entel Ocean estamos convencidos de que nuestro trabajo puede cambiar la forma en que las grandes empresas protegen sus operaciones de negocio, asegurando mantener la vanguardia dentro del mercado en el que se desenvuelven.

Nuestro propósito está focalizado en cambiar paradigmas en ámbitos de ciberseguridad, por lo que contamos con un portafolio de soluciones que se adecúa a las necesidades de nuestros clientes, somos el partner tecnológico de las grandes empresas y **habilitamos un entorno favorable para la transformación digital, generando y protegiendo datos con un equipo de especialistas** innovador y capacitado para los tiempos digitales en el que nos encontramos.

CAPÍTULO 1.
EL CIBERCRIMEN COMO SERVICIO

Así como muchas organizaciones tecnológicas han evolucionado a lo largo de los años para utilizar servicios basados en la nube, los ciberdelincuentes también han adoptado un modelo similar de servicio. Si bien esto puede haber comenzado hace algunos años, la táctica ha seguido creciendo y en la actualidad supone un escenario poco favorable para las operaciones de negocio de las industrias.

En efecto, aprovechando la diversidad **de soluciones de fácil acceso existentes en sitios de mercado negro, la compra de malware como servicio (MaaS) ha conllevado un aumento sustancial en la explotación de vulnerabilidades,** donde ciberdelincuentes sin mayor sofisticación ni conocimientos pueden causar un gran impacto en las operaciones de negocio de las organizaciones.



¿Cómo opera Malware-as-a-Service (MaaS)?

La característica principal es el ofrecimiento del servicio de alquiler de malware, que permite acceso a soluciones personalizables.

Algunos, incluso, ofrecen garantías de devolución de dinero, mientras que otros, operan basados en comisiones vinculadas al éxito de las campañas perpetradas, **que en líneas generales fluctúa entre el 10% a 30% en algunos casos.**

USD $2,000

Es el precio promedio que los compradores están dispuestos a pagar por un exploit en el underground

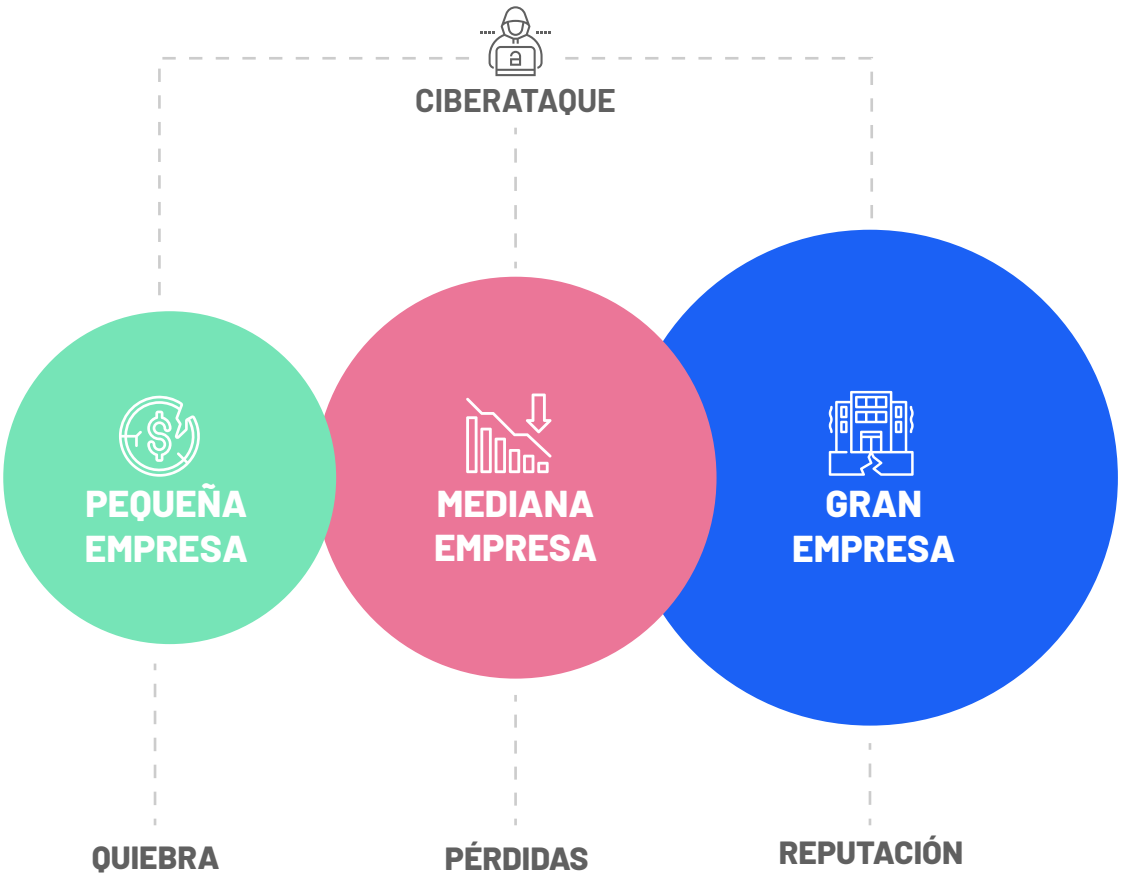
El malware ha pasado a representar una peligrosa fauna cibernética, donde destacan algunos por su capacidad disruptiva, otros por la capacidad de propagación en cortos periodos de tiempo, otros por el tipo de daño reputacional que infringen y otros por aplicar extorsión en sus víctimas con el fin de asegurar sus demandas, principalmente monetarias.

En líneas generales, **el impacto que produce un ciberataque elaborado contra una empresa,** estará relacionado directamente con el tamaño de la misma:

› **Una pequeña empresa** expuesta ante un ciberataque **tiene grandes probabilidades de desaparecer,** debido a que no les es posible solventar interrupciones prolongadas en sus operaciones ni tampoco tienen el capital suficiente como para prepararse ante este tipo de situaciones.

› **Una mediana empresa podría soportar un ciberataque,** ya que posee algunos controles y procesos documentados con planes de contingencia ante hechos disruptivos. **Sin embargo, el impacto sigue siendo casi fatal para su operación.**

› **Una empresa de mayor escala**, que suele tener un equipo especializado en la seguridad de la información y sistemas apoyados por la implementación de marcos metodológicos reconocidos, **está preparada para un eventual incidente** de seguridad, **sin embargo, se producen impactos reputacionales, legales y también pérdidas de productividad que se traducen en riesgos para el negocio.**

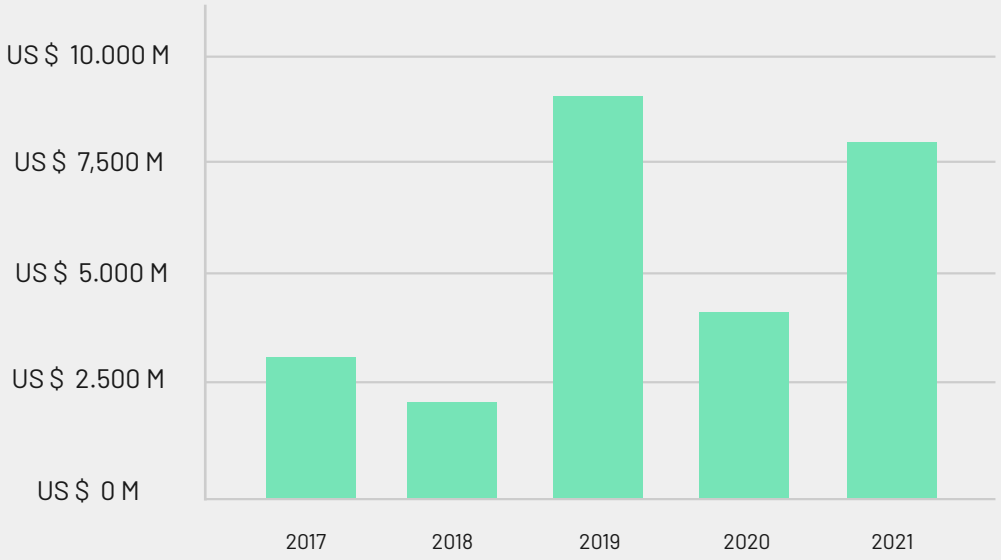


Con base a lo anterior, nos queda preguntarnos si **la ciberseguridad ¿es solo para grandes empresas?**
-La respuesta es un rotundo NO.

Vivimos en tiempos memorables, donde **existen múltiples recursos a medida para todo tipo de requerimientos, inclusive algunos de código abierto que pueden ser implementados en pequeñas organizaciones** (SOHO), pero aquel recurso que puede ayudar a las empresas de forma transversal es la concienciación en términos de ciberseguridad.

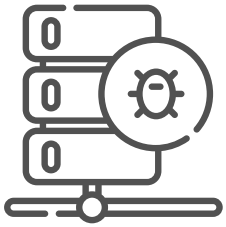
Según estadísticas globales externas, las ciber estafas fueron nuevamente **el delito con mayor recaudación de dinero, alcanzando cifras aproximadas de 7.700 millones de dólares**, seguido por los robos de cuentas bancarias, transacciones en mercados negros y pagos por ransomware. Por lo que, una vez más evidenciamos el factor humano, como la principal brecha de seguridad, y la explotación de la tendencia general de la gente a confiar, como principal vector de entrada de amenazas contra los negocios.

Valores anuales de criptomonedas recibidas por estafadores



Al respecto, recomendamos seguir las normativas internacionales tales como ISO 27001 en su control A.7.2.2 "Concienciación con educación y capacitación en seguridad de la información" o NIST PR.AT-1: "Todos los usuarios se encuentran entrenados e informados", a fin de tener bases para divulgar campañas educativas orientadas al correcto uso de las herramientas tecnológicas, haciendo énfasis en cómo proceder al recibir entradas de orígenes desconocidos, objeto prevenir que sus colaboradores sean víctimas de entes maliciosos y comprometan a sus organizaciones.

› El crecimiento del cibercrimen con Ransomware-as-a-Service



En 2021, la amenaza representada por el ransomware siguió creciendo. La tendencia fue principalmente dirigida contra empresas más grandes debido a que con ello se pretende solicitar pagos más elevados. Sin embargo, otra tendencia importante fue el auge del ransomware como servicio (RaaS), que tuvo un crecimiento abismante respecto a años anteriores.

Siendo parte del modelo MaaS, **Ransomware-as-a-Service se puede definir como aquel modelo de servicios en que los operadores de ransomware permiten a terceros lanzar ataques utilizando su programa malicioso a cambio de una tarifa,** quienes no requieren de mayores niveles de sofisticación ni conocimientos para causar un gran impacto en las operaciones de negocio de las organizaciones.

Si bien, a menudo vimos nombres de empresas afectadas a nivel global con especial hincapié en Estados Unidos y Europa, **el cono Sudamericano no quedó ajeno a estas amenazas, lo que nos lleva a proyectar que 2022 seguirá siendo un año de crecimiento para el cibercrimen,** pero con algunos matices favorables para las industrias principalmente por algunas acciones poco visibles que nos entregó este ya nombrado año del equilibrio.

CAPÍTULO 2.
TAKEDOWN CIBERACTORES

2021 fue el año donde se registró el mayor número de operaciones conjuntas y combinadas contra actores de amenazas y portales de mercado negro.

Este hecho ha generado un ambiente disuasivo que llegó para instaurar un escenario esperanzador, definiendo que los cibercriminales ya no tienen libre albedrío y son objetivo de instituciones gubernamentales que están actuando de forma organizada para sofocar la vertiginosa alza del cibercrimen.

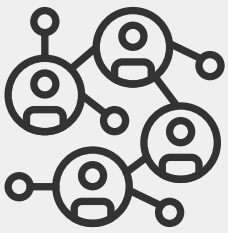
Definiciones importantes

Operaciones Conjuntas:

Aplicación de principios de planificación, organización y administración para la ejecución de tareas en todo el campo de batalla, exigiendo la integración de las energías de la nación, materializadas por la cooperación entre las distintas ramas de las Fuerzas Armadas, así como la de las Organizaciones gubernamentales de carácter civil. Vale decir, operaciones entre instituciones de defensa y orden de un mismo país.

Operaciones Combinadas:

Aplicación de principios de planificación, organización y administración para la ejecución de tareas en las que intervienen fuerzas de varios países.



Existe, por lo tanto, una diferencia substancial entre ambos conceptos, ya que si el primero apunta hacia la necesidad de emplear conjuntamente todos los esfuerzos de que dispone una nación para defenderse, el segundo se orienta a la moderna teoría estratégica de la **defensa colectiva**, esto es, a la necesidad de que cada vez más, la seguridad internacional se apoye en la actuación coordinada de varias naciones.

Una mirada a los hechos

FECHA	AMENAZA	ORGANISMO(S) A CARGO DE LA OPERACIÓN	PAÍS(ES)
ENERO	"Emotet"	EUROPOL & EUROJUST El malware reapareció en noviembre, tardó 10 meses, debido a la necesidad de reinventar nuevos vectores y accesos iniciales de calidad.	Alemania, Ucrania, UK, USA, Países Bajos, Canadá, Francia, Lithuania
ENERO	"Netwalker" ransomware	US DOJ, FBI, Bulgarian National Investigation Service, and Bulgaria's General Directorate Combating Organized Crime	USA, Bulgaria
MAYO	"Le Monde Parallèle" Marketplace	French National Directorate of Intelligence and Customs Investigations	Francia
MAYO	"DarkSide" ransomware	DarkSide decidió cerrar su operación "debido a la presión de EE.UU." y después de perder el acceso a sus servidores públicos.	USA
JUNIO	"AnOn App" Marketplace	Austalian Federal Police + FBI	Australia, USA
JUNIO	"Marketo" Marketplace	EUROPOL	Alemania, Australia, Dinamarca, Moldova, Ucrania, UK (the National Crime Agency), USA (DEA, FBI, and IRS)
JUNIO	"Slilpp" Marketplace	US Department of Justice (DOJ) Activo nuevamente en 2022	US, Alemania, Países Bajos, Rumanía
JUNIO	"DoubleVPN"	Dutch National Police	National Crime Agency, US, EUROPOL, EUROJUST, Países Bajos
JUNIO	Miles de sitios de tiendas falsas de farmacias	INTERPOL "Pangea XIV OP"	INTERPOL
OCTUBRE	"White House Market" Marketplace	WHM Shutdown - Cierre voluntario de la plataforma por parte de su administrador	-
OCTUBRE	"Botnet" (sin antecedentes de su nombre)	La policía ucraniana arresta al operador DDoS que controla 100,000 bots	Ucrania
OCTUBRE	"Trickbot" botnet	Múltiples acciones de interrupción ocurrieron durante Q3 de 2021, pero no tuvieron mayores efectos	Microsoft, Digital Crimes Unit, ESET, Lumen's Black Lotus Labs, NTT Ltd, Broadcom's Symantec enterprise business, Financial Services Information Sharing and Analysis Center (FS-ISAC)
NOVIEMBRE	Red de cibercrimen financiero	INTERPOL "HAECHI-II OPS"	+20 países, entre ellos Colombia

Hitos más importantes

FECHA	HITOS
FEBRERO	El arresto de los miembros de Egregor / Maze en Ucrania.
MARZO	El arresto de un afiliado de GandCrab en Corea del Sur.
JUNIO	El arresto de un grupo de lavadores de dinero ucranianos que trabajaban con el grupo de ransomware Clop.
SEPTIEMBRE	Sanciones contra Suex, un cripto intercambio ruso utilizado para procesar pagos de ransomware.
OCTUBRE	El arresto de 12 sospechosos detrás del ransomware LockerGoga.
OCTUBRE	El arresto de dos operadores de ransomware en Ucrania.
NOVIEMBRE	Dos afiliados de REvil arrestados en Rumania.
NOVIEMBRE	El arresto de un afiliado de GandCrab en Kuwait.
NOVIEMBRE	El arresto de un afiliado de REvil en Ucrania por el ataque de Kaseya.
NOVIEMBRE	La acusación de un afiliado de REvil con sede en Rusia por el ataque de ransomware de 2019 contra los municipios de Texas.
NOVIEMBRE	El arresto de un ejecutivo de cripto intercambio que ayudó al grupo de amenazas Ryuk a lavar sus ganancias.
DICIEMBRE	El arresto de un ciudadano canadiense por el ataque contra un proveedor de atención médica de Alaska.

- Nuevamente, se demuestra que los cibercriminales ya no tienen libre albedrío, potenciado con el hecho de que distintos equipos internacionales de seguridad han mancomunado esfuerzos para desmantelar a estos grupos sofisticados que causan tanto impacto a nivel mundial.

- Es probable que veamos cómo bajan las campañas de malware, al menos por un corto periodo, entendiendo que ningún grupo que trabaje con este tipo de amenaza quiere llegar a ser muy visible para las comunidades.

- Los grupos de actores buscarán la forma de ser más sigilosos en sus operaciones, durante 2021 evidenciamos grupos de ransomware presentes a nivel nacional como Hydra y Haron, quienes pese a ser ransomwares emergentes, se han mantenido en el anonimato debido a la dificultad que supone obtener información de ellos, ya que sus portales cuentan con una capa de autenticación que priva a equipos de seguridad su acceso rápido y por lo mismo, tienen menor impacto mediático en la comunidad.

CAPÍTULO 3.
INFRAESTRUCTURA CRÍTICA

> **"Los ataques a la infraestructura crítica deben tratarse como un problema de seguridad nacional similar al terrorismo"**
>
> DoJ USA (octubre de 2021)

Precisamente durante las últimas décadas hemos visto los impactos disruptivos que genera este tipo de ataques en la sociedad. Casos como el de Estonia (2007), Irán (2010), Ucrania (2015/2016), Arabia Saudita (2017), Chile (2018/2020), EE.UU. (2021), no deben pasar desapercibidos.

› Estonia (2007):

Durante la Segunda Guerra Mundial los soviéticos entraron a Estonia para erradicar a los Nazis, sin embargo, esta ocupación perduró hasta 1991, periodo en el cual se erigió un monumento a los soldados soviéticos caídos en el centro de la ciudad, que para los estonios, representaba nada más que la ocupación soviética de esos años.

En abril de 2007, los gobernadores de Estonia decidieron trasladar dicha estatua hacia un cementerio de soldados de la Guerra, lo cual para los rusos significó un insulto a sus héroes. Debido a que en el país aún quedaban miles de rusos que se encontraban arraigados en el país, hubo una revuelta civil que se levantó protestando contra esta decisión.

No obstante, la estatua fue trasladada en la madrugada del 27 de abril de 2007. Esa misma mañana, las páginas web del gobierno comenzaron a fallar y el acceso a la banca online se bloqueó.

Estonia estaba siendo víctima de un ataque de DDoS, haciendo que todos sus servicios estuviesen colapsados de peticiones sin poder operar. Los ciberataques proliferaron durante las siguientes dos semanas, incomunicando al país del resto del mundo, con serias deficiencias en los servicios públicos, marcando un precedente en la historia de la ciberseguridad debido a que no sabían de dónde provenían los ataques ni como responder ante ellos. Pero aunque lo supieran, el problema estaba en ¿qué se podría haber hecho para evitarlo?, ¿cuáles eran las reglas de enfrentamiento de este nuevo tipo de conflicto asimétrico? Esta fue la primera vez que se utilizó internet como arma para perturbar el funcionamiento de una nación, sentando bases para que múltiples naciones planificaran sus defensas en este nuevo escenario de conflictos asimétricos.

Irán (2010): Stuxnet

En enero de 2010, inspectores de la Agencia Internacional de Energía Atómica notaron con desconcierto que las centrifugadoras de la planta nuclear en Natanz, en Irán, usadas para enriquecer uranio, estaban fallando, ante lo cual no encontraban explicación. El fenómeno se repitió cinco meses después en el país, pero esta vez los expertos pudieron detectar la causa: un malware creado específicamente para estos fines, con un código 20 veces más complejo que cualquier otro conocido.

El malware - ahora conocido como Stuxnet - tomó el control de al menos 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse. Fue la primera vez que un ataque cibernético logró dañar la infraestructura del "mundo real", Stuxnet fue la primera arma creada completamente de código de programación.

Nueve meses posteriores a su detección, esta "arma" que puede quebrar redes eléctricas, destruir oleoductos y muchos otros daños en infraestructura crítica estuvo disponible en mercados negros para que cualquiera pudiera descargarla y desamblarla, con videos que explicaban paso a paso cómo se creó esta innovadora herramienta a base de código.

Ucrania (2015 / 2016): BlackEnergy / Industroyer

Durante diciembre de 2015 y nuevamente en diciembre de 2016, se vivieron horas complejas en Ucrania debido a ciberataques dirigidos - conocidos como BlackEnergy e Industroyer, respectivamente - los que afectaron a las redes eléctricas de este país.

Estos apagones fueron los primeros en el mundo que se documentaron como producidos por el uso de un código malicioso.

Arabia Saudita (2017): Triton

El malware conocido como Triton se usó para sabotear una planta petroquímica ubicada en Arabia Saudita. Fue diseñado para afectar a los controladores del Sistema de Instrumentos de Seguridad Triconex de Schneider Electric, con el objetivo de dañar la instalación o hacer que explotara. Afortunadamente, los expertos de ciberseguridad lograron responder a tiempo ante este incidente.

Chile (2018 / 2020): Lazarus Group / Sodinokibi ransomware

El memorable caso que afectó al Banco de Chile en el año 2018, donde el grupo de actores de amenaza norcoreanos lograron extraer US$10 millones de dólares en transacciones autorizadas. Este incidente fue uno más de la campaña de estos sofisticados ciberactores, quienes entre 2014 y 2021 han afectado a instituciones financieras en al menos 13 países. Se cree que los ingresos se destinan al desarrollo de tecnología nuclear y de misiles de Corea del Norte.

Por otra parte, en 2020 el ransomware REvil (a.k.a. Sodinokibi) afectó a Banco Estado, institución que mantuvo la mayoría de sus sucursales cerradas por al menos 4 días, causando indisponibilidad en sus sistemas y atención a clientes. Posterior a estos incidentes, la Comisión de Economía acordó solicitar al Ejecutivo poner suma urgencia al mensaje en segundo trámite que **establece normas sobre delitos informáticos, que deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.**

EE.UU. (2021): Ransomware DarkSide

En mayo de 2021, Colonial Pipeline, una empresa que proporciona aproximadamente el 45% de los suministros de combustible de la costa este de Estados Unidos, se vio obligada a cerrar sus operaciones durante casi una semana tras el cifrado de sus sistemas debido al RaaS Darkside. La compañía habría efectuado el pago de casi US$4,4 millones en criptomonedas, lo inédito: el FBI logró recuperar US$2,3 millones de ese pago.

¿Cómo avanzamos en materias de resguardo de infraestructuras críticas en Chile?

De acuerdo con lo estipulado en la Política Nacional de Ciberseguridad (PNCS) promulgada en 2017, se identifica y jerarquiza las infraestructuras críticas de la información (ICI) señalando:

> *"Los sectores que componen la clasificación de ICI son muy similares y se repiten en varias clasificaciones a nivel internacional. En el caso chileno,* ***mientras se adopta una política específica para infraestructuras críticas****, la infraestructura de la información de los siguientes sectores será considerada como crítica:* ***energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras."***

La PNCS, se basa en una visión que apunta al año 2022, para conseguir el objetivo de contar con un ciberespacio libre, abierto, seguro y resiliente. Los avances en la materia a nivel nacional pueden observarse en el último estudio de la International Telecommunication Union (ITU), donde **Chile se ubica en la posición 74 del ranking internacional en ciberseguridad y la posición 7 del continente Americano.**

Gracias a estas iniciativas se han creado nuevos roles en organismos públicos que tienen la responsabilidad de regular, auditar, fiscalizar y sancionar cuando corresponda a ciertos sectores privados, trabajo que ha sido coordinado por la División de Redes y Seguridad Informática del Ministerio del Interior, que dentro de sus áreas y funciones tiene al CSIRT de Gobierno, que, por un lado, se encarga de la seguridad del Estado y, por otro lado, se hace cargo de estos roles en el sector privado.

Sistemas de control industrial (ICS)

Los Sistemas de Control Industrial son utilizados en múltiples servicios esenciales y vitales para el funcionamiento de la sociedad. **Las organizaciones industriales dependen mayoritariamente de las tecnologías operativas (OT).**

La tecnología operativa es el uso de hardware y software para monitorear y controlar los procesos físicos, los dispositivos y la infraestructura. Los sistemas de tecnología operativa se encuentran en una amplia gama de sectores con alta utilización de activos, realizando una gran variedad de tareas que van desde el monitoreo de infraestructura crítica hasta el control de máquinas en una planta de fabricación.

La denominada "Industria 4.0", requiere sistemas de tecnología de la información (IT) para identificar problemas o aumentar la eficiencia de los sistemas de tecnología operativa. Sin embargo, la conexión a Internet de una red de OT a través de una red IT, expone inmediatamente la red y todos sus dispositivos, a todo el panorama de amenazas.

El riesgo se incrementa debido a que las redes OT generalmente no están protegidas, ya que fueron diseñadas originalmente con el supuesto de que no estarían expuestas. En líneas generales es tecnología antigua y heredada. Otro punto de riesgo radica en el aumento del acceso remoto a las redes de OT por parte de proveedores externos, lo que amplía aún más la superficie de ataque y crea nuevas brechas de seguridad.

Un reto crucial de la industria 4.0 es la convergencia IT - OT, organizando en todo momento el intercambio de datos e información, de manera estandarizada y segura, entre dispositivos, máquinas, sistemas y servicios.

El proceso de convergencia IT-OT debe contar con diferentes enfoques de ciberseguridad, entendiendo que el entorno IT tiene su orientación hacia la protección de la información, y en el caso del entorno OT se prioriza la continuidad operacional y la protección de los activos físicos.

FACTORES DE RIESGO

- Interconexión de los sistemas de control industrial con sistemas TI tradicionales.
- Acceso a datos del proceso desde cualquier ubicación.
- Sistemas de control industrial conectados a internet.
- Profesionales de seguridad que no son involucrados en el diseño y mantenimiento del sistema.
- Falta de procesos y herramientas de seguridad.
- Uso de tecnologías de TI de propósito general, como TCP/IP.
- Inexistencia de un marco regulador o política de seguridad.

Algunos controles de seguridad básicos:

Software heredado	Configuración predeterminada	Cifrado
Los sistemas OT funcionan con softwares heredados que carecen de suficientes funciones de autenticación del sistema y del usuario, verificación de la autenticidad de los datos o verificación de la integridad de los datos que permitan a los atacantes el acceso incontrolado a los sistemas.	Los sistemas listos para usar con contraseñas simples o predeterminadas y configuraciones básicas facilitan a los atacantes enumerar y comprometer los sistemas OT.	Los sistemas listos para usar con contraseñas simples o predeterminadas y configuraciones básicas facilitan a los atacantes enumerar y comprometer los sistemas OT.
Políticas de acceso remoto	**Políticas y procedimientos**	**Segementación de la red**
Los sistemas SCADA conectados a troncales no auditados o servidores de acceso remoto brindan a los atacantes un conveniente acceso de puerta trasera a la red OT, así como a la LAN corporativa.	Se crean brechas de seguridad cuando el personal de TI y OT difieren en su enfoque para asegurar los controles industriales. Las diferentes partes deben trabajar juntas para crear un política de seguridad unificada que proteja tanto la tecnología de TI como de OT.	La red OT plana y mal configurada conectada a internet, las funciones de firewall que no detectan o bloquean la actividad maliciosa brindan a los atacantes un medio para acceder a los sistemas OT.
Ataques DDoS	**Ataques a aplicaciones web**	**Malware**
Las fuentes invalidadas y los controles de acceso limitados permiten a los atacantes que intentan sabotear los sistemas OT ejecutar ataques DoS en sistemas vulnerables sin parches.	Los sistemas OT tradicionales, incluídas las HMI y las computadoras lógicas programables (PLC), están cada vez más conectados a la red y son accesibles desde cualquier lugar a través de la interfza web. Los sistemas desprotegidos son vulnerables a los ataques SQL Injection y cross-site scripting.	Los sistemas OT son vulnerables a los ataques y deben incorporar protección antimalware, controles de firewall basados en host y políticas de administración de parches para reducir la exposición.

CAPÍTULO 4.
ROBO DE INFORMACIÓN

> **“Las cifras, los costos y los impactos de la filtración de datos aumentaron en 2021”**

El escenario actual nos ha llevado a normalizar una condición de trabajo: enfrentarnos diariamente contra múltiples amenazas cibernéticas.

Al igual que años anteriores, **2021 estuvo marcado por noticias de filtraciones de credenciales de grandes organizaciones como Facebook, LinkedIn, Twitter,** el Registro Nacional de las Personas de Argentina, el Instituto Nacional Electoral de México, **Software electoral de Israel, entre muchos otros,** como también de un millar de personas individualizadas quienes dejaron en evidencia la falta de conciencia digital en el manejo de sus credenciales.

En la actualidad, las organizaciones se ven en la necesidad de aplicar controles de seguridad contra múltiples campañas maliciosas que buscan aprovechar cualquier brecha de seguridad existente en las redes. Es por ello que cobra importancia **contar con el conocimiento y herramientas que nos puedan permitir disminuir estas brechas de seguridad y aumentar nuestras capas de protección frente a estas amenazas.**

“Debemos crear una cultura y un ecosistema proactivo frente a temas de seguridad”

Uno de los casos más connotados de robo y filtración de información, ocurrió el 2 de febrero, donde se registró el mayor leak de la historia que fue bautizado como **PWCOMB21.**

PWCOMB21 (PassWord Compilation Of Many Breaches Of 2021) es la mayor compilación de filtraciones de credenciales de todos los tiempos, con más de 3.280 millones de registros obtenidos de múltiples filtraciones de diferentes empresas y organizaciones que sucedieron a lo largo de los años, concentradas en solo un archivo organizado por correo electrónico, nombre de usuario y contraseña.

La filtración no solo expone credenciales actuales o pasadas, sino que también brinda información sobre los elementos y patrones clave de las contraseñas junto a algunos hábitos de reutilización; es un banco de información sin precedentes. En muchos casos, existen hasta 30 contraseñas vinculadas a un único correo electrónico, dejando expuestos a aquellos usuarios con hábitos de reutilizar contraseñas.

3.280 millones	2.180 millones	26 millones
Total de contraseñas expuestas: 3.279.064.312	Total de correos filtrados	Total de dominios filtrados
100 GB	1,5 millones	625.505
Tamaño de base de datos de contraseñas descomprimidas	Total de contraseñas de gobiernos espuestas: 1.502.909	Total de contraseñas de gobiernos espuestas: 625.505
18,6 GB (7Z)		
Tamaño de base de datos de contraseñas comprimidas		

En Chile +5800 credenciales asociadas a sitios gubernamentales fueron develadas.

País	Total de credenciales expuestas
Estados Unidos de América (*.gov)	625.505
Reino Unido (*.gov.uk)	205.099
Australia (*.gov.au)	136.025
- - -	- - -
Brasil (*.gov.br)	68.535
México (*.gov.mx)	31.995
Argentina (*.gov.ar)	15.604
Colombia (*.gov.co)	9.428
Perú (*.gob.pe)	6.038
Chile (*.gob.cl)	5.843
Costa Rica (*.go.cr)	4.402
Ecuador (*.gov.ec)	2.792
El Salvador (*.gob.sv)	1.640
Venezuela (*.gob.ve)	1.461
Total mundial	**1.502.909**

¿Quiénes están detrás de este tipo de amenaza y qué impactos supone?

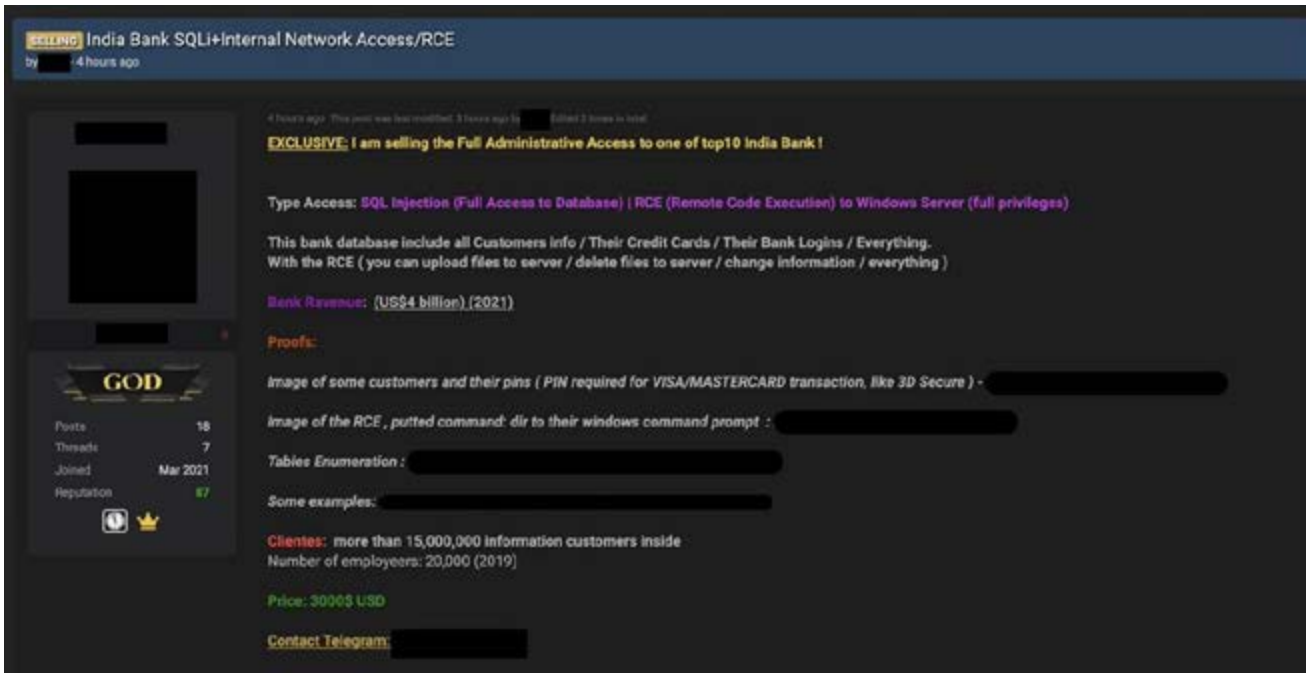
La respuesta es clara: malware infostealer y variantes de ransomware que han adoptado la estrategia de robo de datos y extorsión.

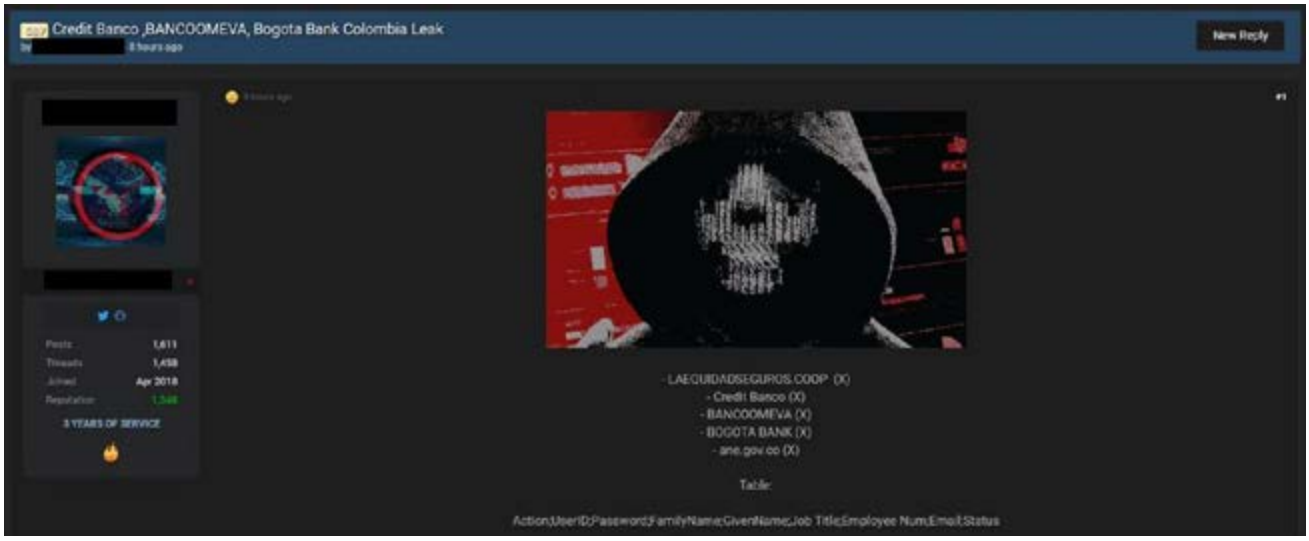
Infostealers, es el nombre genérico de programas informáticos maliciosos que se introducen a través de internet en un ordenador con el propósito de obtener de forma fraudulenta información confidencial del propietario, credenciales de acceso a sitios web, contraseñas, números de tarjetas bancarias o documentos con información clasificada. Asimismo, destacamos que gran parte de las variantes de este tipo de malware se comercializa por mercados negros siguiendo el modelo de Malware-as-a-Service.

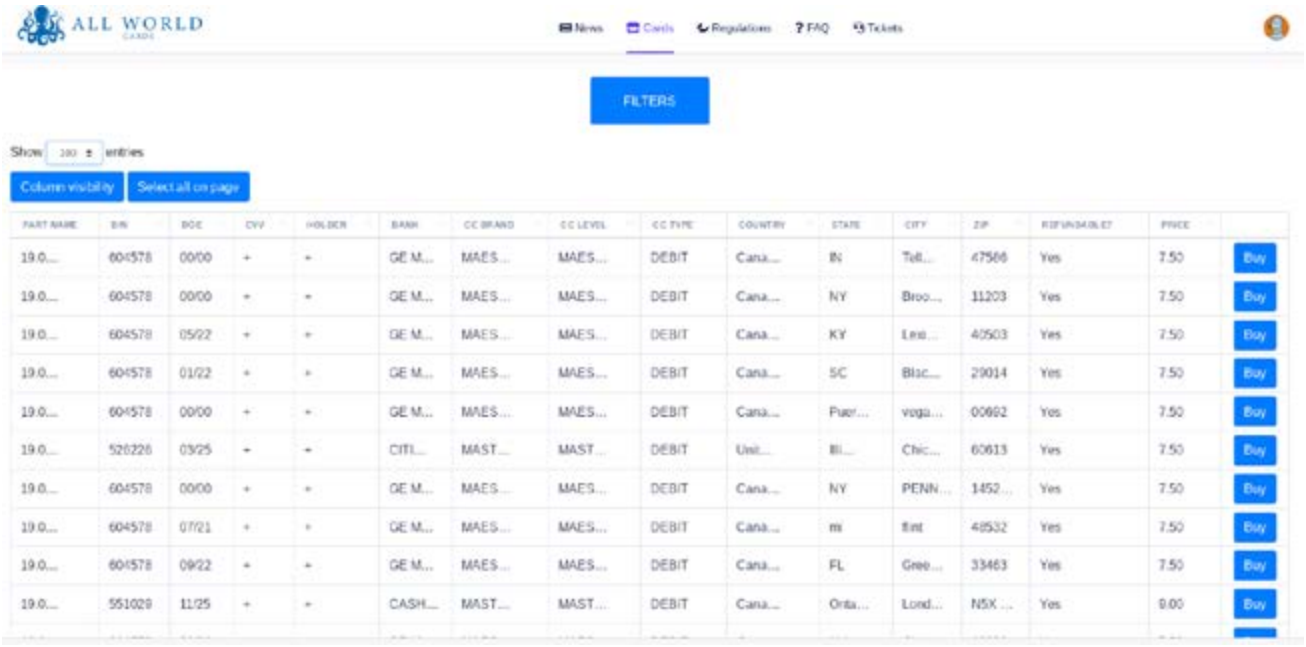
En conclusión, su intención principalmente es lograr obtener todo lo que pueda utilizar para cumplir con las principales motivaciones de este tipo de campañas:

- Recompensa Económica
- Espionaje
- Ventaja corporativa o política

Uno de los patrones comunes es la utilización de mercados negros para comercializar este tipo de datos, aludiendo a la reutilización de credenciales para apoyar otras campañas ofensivas contra las mismas organizaciones, o simplemente, ofreciendo medios digitales para la adquisición de bienes a través de carding (venta de tarjetas bancarias o tarjetas de comercios prepagadas).







En 2021, el robo de credenciales fue la principal causa raíz de los incidentes de ciberseguridad. Al mismo tiempo, debido a que en la mayoría de los casos se puede identificar los datos personales de la víctima, es que esta actividad resulta tan rentable, puesto que:

Una filtración no solo expone credenciales actuales o pasadas, sino que también brinda información sobre los elementos y patrones clave de las contraseñas junto a algunos hábitos de reutilización; es un banco de información sin precedentes que puede dejar expuestos a aquellos usuarios con malos hábitos respecto a la "reutilización de contraseñas".

Según estadísticas recopiladas en distintas empresas nacionales, el 84% de las personas admite que reutiliza contraseñas en varias de sus cuentas, lo que dispara los indicadores de riesgo para las empresas.

Para poder apalancar en gran medida este tipo de amenazas, recomendamos proteger las identidades con **múltiples factores de autenticación,** como también instaurar el hábito de **no almacenar credenciales en los navegadores de internet,** sino que en su reemplazo se recomienda **utilizar gestores de credenciales,** tales como Keepass. Es imperante adoptar los nuevos enfoques de la ciberseguridad.

Para mayores detalles https://www.keepass.info

Controles de autenticación

La autenticación sólida es la primera línea de defensa en la batalla para proteger los recursos de la red, los procesos que respaldan este requisito se conocen como administración de identidad y acceso (IAM).

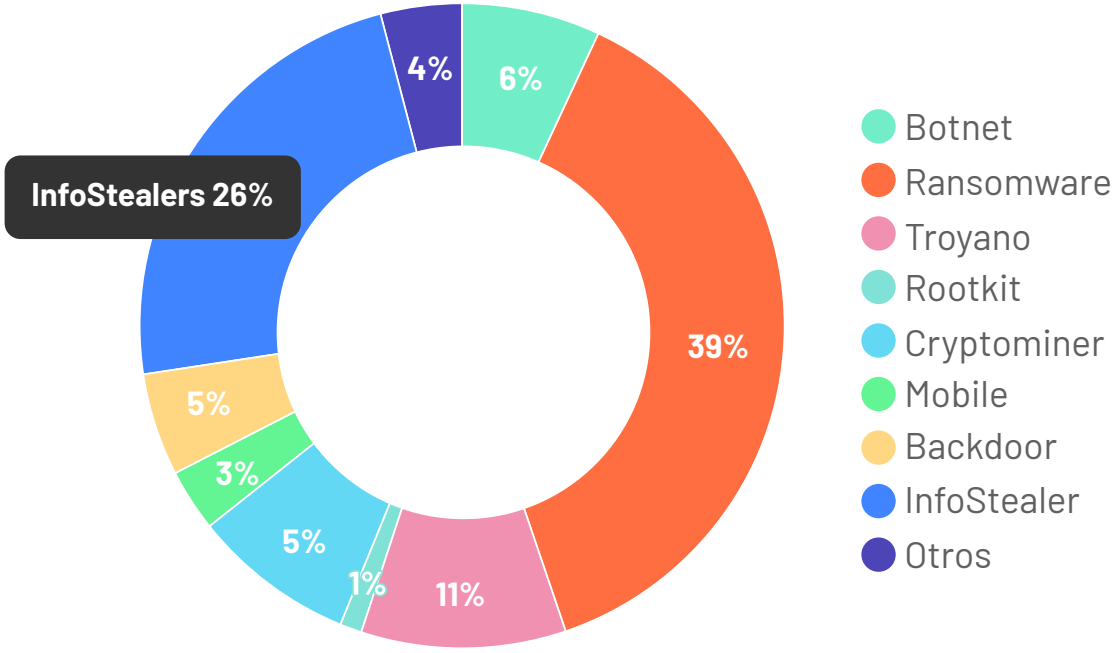
Dentro de IAM, las tecnologías de autenticación aseguran que sólo los sujetos válidos (usuarios o dispositivos) puedan operar una cuenta. Pero la autenticación no es un proceso único; existen muchos métodos y mecanismos diferentes, algunos de los cuales se pueden combinar para formar productos más efectivos. Un sistema de administración de identidad y acceso (IAM) generalmente se describe en términos de cuatro procesos principales:

- **Identificación:** creación de una cuenta o ID que represente de manera única al usuario, dispositivo o proceso en la red.
- **Autenticación:** probar que un sujeto es quién o qué dice ser cuando intenta acceder al recurso.
- **Autorización:** determinar qué derechos deben tener los sujetos sobre cada recurso y hacer cumplir esos derechos.
- **Accounting (Registros):** seguimiento del uso autorizado de un recurso o uso de derechos por parte de un sujeto y alertas cuando se detecta o intenta un uso no autorizado.

Ya no existe una red física, todo se migra aceleradamente a las nubes. Por lo tanto, **¿cómo podemos proteger los activos que no están en nuestra red física?** Esta interrogante es la que marcó la pauta en 2021, redes cada vez más descentralizadas donde los controles de autenticación, fueron la prioridad para la seguridad, entendiendo que cada usuario inicia sesión en diferentes plataformas o aplicativos.

Esta situación ha dejado un escenario poco favorable para aquellas empresas que no cuentan con políticas y buenas prácticas de seguridad. Muchos de estos portales expuestos a Internet, sufren constantes ataques que no son advertidos por los administradores.

Debido al ya mencionado Malware-as-a-Service **Infostealer**, capaz de obtener distintas credenciales directamente desde terminales comprometidos, **ya no basta pensar en contraseñas complejas, ni aquellas con más de 14 caracteres.** Todos los años vemos nuevas estadísticas que nos demuestran la facilidad con que los actores de amenazas podrían "romper" un sistema de autenticación por credenciales "poco robustas". En la actualidad éstas son extraídas en texto plano directamente de los terminales comprometidos: ¿qué sentido tiene entonces?



Destacamos la presencia de distintas variantes de malware infostealer a nivel nacional, junto con el robo de credenciales y el comercio ilegal que suponen en foros de mercado negro en el underground.

En conclusión, ya no basta tan sólo en concentrarse con tener una contraseña robusta: las campañas de phishing, la presencia activa de malware infostealers a nivel nacional y la falta de concienciación, son los factores claves a abordar para la protección de identidades. Si no tomamos acciones inmediatas, no habrá método o tecnología que evite un ataque.

Por tanto, si conocemos este nuevo escenario, ¿cómo nos debemos proteger? ¿Estamos dispuestos a seguir exponiendo nuestros activos de información?

Las estrategias actuales se basan en el entendimiento de estas amenazas, implementando metodologías capaces de minimizar las brechas de seguridad existentes con la integración de diversos métodos de autenticación.

La autenticación como elemento clave de seguridad

Autenticación se puede definir como la capacidad de identificar y demostrar de forma exclusiva que un usuario es realmente quién asegura ser. Para poder lograr esta autenticación existen diferentes métodos que se pueden usar tanto de forma individual ("autenticación simple") o combinando dos o más métodos diferentes (múltiple factor de autenticación). Con el MFA, si un factor se ve comprometido, un atacante todavía tiene que romper al menos una barrera más antes de poder acceder a la cuenta del objetivo.

¿Cómo funciona la autenticación multifactorial?

La autenticación de múltiples factores (MFA) utiliza diferentes tecnologías para autenticar la identidad de un usuario. En cambio, la autenticación de un solo factor utiliza una sola tecnología para probar la autenticidad del usuario. Con el MFA, los usuarios deben combinar tecnologías de verificación de al menos dos grupos o factores de autenticación diferentes. Estos factores se dividen en tres categorías: algo que conoces, algo que tienes y algo que eres.

Factores de autenticación

Algo que se conoce
(factor de conocimiento)

- Contraseñas o Pin

› Algo que conoces (factor de conocimiento):

Suele ser una contraseña, un PIN o una frase de paso, o un conjunto de preguntas de seguridad y sus correspondientes respuestas que sólo conoce la persona. Para utilizar un factor de conocimiento para MFA, el usuario final debe introducir correctamente la información que coincida con los detalles que se almacenaron previamente en la aplicación en línea.

Algo que tienes
(factor de posesión)

- Mensaje de texto SMS
- Aplicaciones de Tokens

› Algo que tienes (factor de posesión):

Pueden ser dispositivos que generan tokens cada cierto tiempo, tarjetas de coordenadas, aplicaciones de autenticación para celulares que generan claves de segur idad OTP (One-Time Password), o códigos que llegan a tu teléfono por mensaje de texto o a tu correo electrónico con un tiempo limitado de duración.

Algo que usted es
(factor de inherencia)

- Huellas dactilares
- Reconocimiento facial

› Algo que eres (factor de inherencia):

Los datos biométricos sobre un individuo van desde las huellas dactilares, los escaneos de retina, el reconocimiento facial y el reconocimiento de voz hasta los comportamientos (como la intensidad o la rapidez con que la persona teclea o desliza el dedo en una pantalla). Este suele ser el factor con mayor poder y capacidad de frenar una vulneración de tus cuentas, porque es algo que a los actores de amenazas les es más complejo conseguir.

Fuente: Entel Ocean https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1078/

A fines de agosto de 2021, la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE.UU. (CISA, por sus siglas en inglés) agregó la autenticación de un solo factor a la lista de malas prácticas de ciberseguridad "excepcionalmente riesgosas" que podrían exponer la infraestructura crítica, así como las entidades gubernamentales y del sector privado, a ataques cibernéticos devastadores. De esta forma, la lista mantiene 3 entradas principales:

1. Uso de software deprecado o al final de su vida útil.
2. Uso de contraseñas y credenciales conocidas/por defecto/predeterminadas.
3. Uso de autenticación de un solo factor para el acceso remoto o administrativo a los sistemas.

Del mismo modo, a pesar de los años de esfuerzos promocionales para lograr crear hábitos respecto a la implementación de mecanismos de autenticación múltiples, Microsoft dijo que sólo el 22% de sus clientes empresariales en Azure Active Directory (AD) han adoptado una solución multifactorial para proteger sus cuentas.

MFA es la solución más simple que se puede ofrecer a los usuarios para bloquear ataques de fuerza bruta e intentos de phishing por correo electrónico, los cuales sabemos que se han incrementado a números récord el año pasado.

“Desde enero de 2021 hasta diciembre de 2021, bloqueamos más de 25,6 mil millones de ataques de autenticación de fuerza bruta de Azure AD e interceptamos 35,7 mil millones de correos electrónicos de phishing”

Microsoft

Enfoques de la ciberseguridad actuales

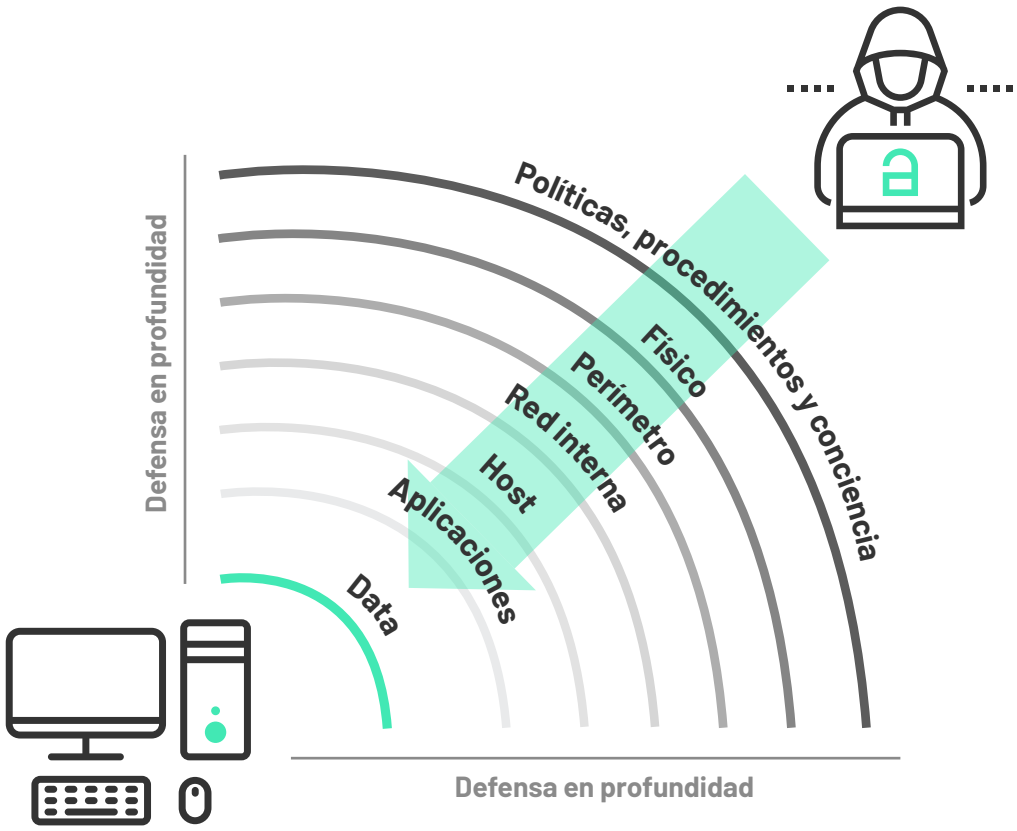
Para las organizaciones que buscan mejorar su postura de seguridad y protegerse contra amenazas más frecuentes y accesibles, una solución de seguridad en capas y autenticación multifactor son fundamentales. Los ciberdelincuentes a menudo apuntarán a aquellas organizaciones más fáciles de comprometer. Al requerir una capa adicional de verificación junto con contraseñas seguras y únicas, es menos probable que las organizaciones enfrenten un compromiso en sus sistemas.

También es aconsejable implementar un enfoque de defensa en profundidad en capas que incluya protección contra malware, parches oportunos, seguridad de DNS, cifrado y copia de seguridad. Sin embargo, quizás el método más eficaz para bloquear el malware sea la educación y la formación. La gran mayoría de las infecciones son causadas por empleados que hacen clic en enlaces incorrectos o tienen malas prácticas de contraseñas que facilitan que los delincuentes entren por la puerta principal, pero la educación ayuda a las personas a detectar intentos y otros métodos de ingeniería social.

Referencias:
https://www.cisa.gov/uscert/ncas/current-activity/2021/08/30/cisa-adds-single-factor-authentication-list-bad-practices
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

Debido a que el ciberdelito siempre está evolucionando, no existe una solución perfecta. Sin embargo, las organizaciones que adoptan un marco de defensa en profundidad y tienen un plan de contingencia para hacer frente a un ataque tienen menos probabilidades de enfrentarse a un ataque costoso y debilitante.

Este concepto se conoce como **defensa en profundidad**



Fuente: https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1078/

Para esto debemos buscar romper el paradigma del perímetro de seguridad tradicional y priorizar la seguridad de la Identidad (Identity-first Security) transfiriendo al nuevo perímetro un enfoque de defensa en profundidad, con herramientas, procesos, seguimiento y políticas integradas.

Nuestra visión y recomendaciones

Es importante que comencemos a rediseñar la forma de abordar la ciberseguridad, los enfoques existentes para las arquitecturas de identidad y seguridad no son suficientes para lograr satisfacer las demandas que se modifican aceleradamente en la actualidad, principalmente impulsadas por la expansión de la superficie de ataque.

Gartner en su reciente reporte de tendencias de seguridad y gestión de riesgos considera que **CyberSecurity Mesh** es una de las principales y más relevantes tendencias tecnológicas, la cual a grandes rasgos considera:

- Inteligenica y analiticas de Seguridad
- Seguridad para la identidad distribuida
- Gestión consolidada de políticas y posturas
- Panales consolidados e integrados.

La tendencia CyberSecurity Mesh nos propone rediseñar el perímetro con una visión de malla de ciberseguridad basada principalmente en la identidad, combinando tendencias de años anteriores que efectivamente nos ayudaron por separado a resolver problemáticas de accesos y confianza, **SASE & Zero Trust** respectivamente, que ahora nos invita a integrar y consolidar bajo una arquitectura de malla de ciberseguridad.

Fuente:
https://portal.cci-entel.cl/Threat_Intelligence/Boletines/1171

CAPÍTULO 5.
PANORAMA VULS

En efecto, en noviembre de 2021, la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos **(CISA-US)**, emitió la directiva operacional **BOD 22-01**, la cual tiene por objetivo **reducir el significativo riesgo que supone la explotación de vulnerabilidades conocidas.**

Referencia: https://cyber.dhs.gov/bod/22-01

Esta directiva se aplica a todo el software y el hardware que se encuentran en los sistemas de información federales administrados en las instalaciones de la Agencia o alojados por terceros.

Lo memorable, fueron los tiempos que se otorgaron para su implementación:

1. Dentro de los 60 días posteriores a la emisión, las agencias revisarán y actualizarán los procedimientos internos de gestión de vulnerabilidades de la agencia de acuerdo con esta Directiva.

2. Remediar cada vulnerabilidad de acuerdo con los plazos establecidos en el catálogo de vulnerabilidades administrado por CISA con un plazo dentro de 6 meses para las vulnerabilidades con una identificación (CVE) asignada antes de 2021 y dentro de dos semanas para todas las demás. Estos plazos predeterminados podrán ser ajustados en caso de grave riesgo para la Agencia Federal.

Esto marca un precedente dentro de los hitos de la ciberseguridad debido a que en la actualidad.

En promedio, el tiempo de parcheo para sistemas expuestos a Internet es de 70 días desde que se libera la actualización de seguridad

La industria digitalizada debe buscar nuevas prácticas de seguridad y defensas contra amenazas que están a la par con las nuevas tecnologías, con una mirada global, partiendo desde la seguridad física hasta la ciberseguridad de forma integral, entendiendo que los controles actuales de seguridad implementados son insuficientes. Estamos en una era de nuevos eventos cada vez más sofisticados por parte de ciber actores maliciosos y que con acciones preventivas oportunas es posible impedir potenciales colapsos.

Referencias:
https://www.cisa.gov/uscert/ncas/current-activity/2021/11/03/cisa-issues-bod-22-01-reducing-significant-risk-known-exploited

¿Por dónde debemos fortalecer el resguardo de nuestros sistemas y proteger nuestros datos?

Gran parte de la explotación de vulnerabilidades evidenciada a la fecha, se ha gestado por una falta de mitigación oportuna. En efecto, a nivel nacional, hemos logrado colectar estadísticas que han demostrado un escenario desfavorable para Chile.

Menos del 16% de las vulnerabilidades se corrigen dentro de los 7 días posteriores a la notificación por parte de las marcas.

- Menos del 41% de las empresas tienen políticas maduras para el parcheado de su infraestructura, esto quiere decir que más de la mitad de las organizaciones no están aplicando las actualizaciones necesarias de sistemas y plataformas en sus infraestructuras, lo que deja un importante campo abierto sin protección, favoreciendo a que ciber actores maliciosos logren explotar estas vulnerabilidades con las consecuencias ya advertidas.

A estas brechas, se añaden lo particular de estos dos últimos años tensionados por la pandemia, empresas principiando en la modalidad de teletrabajo y a la disminución de personal en algunos equipos: un escenario perfecto para atacar a los más desprevenidos.

2021

25 de ene.
2021

Explot SAP Solution Manager (SolMan)

Vulnerabilidad de preautorización de gravedad máxima, la cual podría llevar a la toma de control de sistemas SAP sin parche. La vulnerabilidad fue revelada y parcheada por SAP en marzo de 2020, sin embargo, en enero de 2021 se publicó un código de explotación que redujo de manera drástica la complejidad del ataque para un usuario no autenticado y su explotación se acrecentó mundialmente.

CVE-2020-6207 CVSS: 9.8

Sudo Linux: Baron Samedit

Esta vulnerabilidad apunta a que el comando "sudo" contiene un error que puede resultar en un desbordamiento del búfer permitiendo un escalamiento de privilegios hasta "root". Es decir, entrega el control total y compromete al equipo y sistemas de la víctima si cae en las manos equivocadas.

CVE-2021-3156 CVSS: 7.8

26 de ene.
2021

COMB21: el mayor leak de la historia

02 de feb.
2021

PWCOMB21 (PassWord Compilation Of Many Breaches Of 2021) es la mayor compilación de filtraciones de credenciales de todos los tiempos, con más de 3,280 millones de registros obtenidos de múltiples filtraciones de diferentes empresas y organizaciones que sucedieron a lo largo de los años.

VMWare Vcenter

Tres vulnerabilidades que afectan a vSphere Client y a ESXi, las cuales al ser explotadas permitían a un atacante ejecutar comandos de código remoto (CVE-2021-21972 y CVE-2021-21973), obtener información sensible del sistema al ejecutar una solicitud específica al servidor (SSRF: Server Side Request Forgery).

CVE-2021-21972 CVSS: 9.8
CVE-2021-21973 CVSS: 5.3
CVE-2021-21974 CVSS: 8.8

23 de feb.
2021

Microsoft Exchange: ProxyLogon

02 de mar.
2021

Microsoft publicó una actualización urgente y fuera de ciclo para Exchange Server (on-premise) en respuest a que se detectó ataques activos por actores de amenazas sofisticados a nivel mundial. Las actualizaciones cubren cuatro vulnerabilidades graves que combinadas permiten acceso completo al servidor, permitiendo la instalación de puertas traseras basadas en webshells para facilitar el acceso persistente.

CVE-2021-26855 CVSS: 9.8 CVE-2021-26858 CVSS: 7.8
CVE-2021-26857 CVSS: 7.8 CVE-2021-27065 CVSS: 7.8

F5 BIG-IP & BIG-IQ: REST In IControl

Vulnerabilidad parcheada el 10 de marzo cuya explotación estuvo presente activamente hasta fines de abril. Un actor no autenticado que esté dentro de la red podría realizar la ejecución remota de comandos, esto afecta a la interfaz REST de iControl permitiendo crear o eliminar archivos y deshabilitar servicios sin la necesidad de autenticarse en su infraestructura.

CVE-2021-22986 CVSS: 9.8

10 de mar.
2021

OpenSSL

Esta vulnerabilidad tiene el potencial de bloquear un servicio OpenSSL con un mensaje ClientHello de renegociación creado con fines malintencionados. Esto producirá un quiebre en la referencia de puntero ya que se vincula a unobjeto NULL, lo que provocará un bloqueo y un posible ataque de denegración de servicio. Actualmente en Chile hay más de 1,400 (CVE-2021-3449) Y 130 (CVE-2021-3450) activos afectos a estas vulnerabilidades respectivamente.

CVE-2021-3449 CVSS: 5.9 CVE-2021-3450 CVSS: 7.4

25 de mar.
2021

Backdoor en el código fuente PHP

El equipo de desarrollo de PHP evidencio cambios en su repositorio interno de Git del lenguaje de programación, identificado que se habían efectuado dos modificaciones válidas que lograron agregar una puerta trasera al código fuente en un ataque que tuvo lugar el domingo 28 de marzo. Afortunadamente, este comportamiento fue detectado a tiempo y ya han corregido estas brechas de seguridad.

29 de mar.
2021

Continúa la explotación de SAP

Vulnerabilidades que permiten: "Reconocimiento", "Preautorización de gravedad máxima", "Escalamiento de privilegios y ejecución de comandos arbitrarios", "Activación de estados de denegación de servicio (DoS)" y "Ejecución de comandos del sistema operativo para acceder a la aplicación SAP y a la base de datos conectada".

CVE-2020-6287 CVSS: 10
CVE-2018-2380 CVSS: 6.6
CVE-2016-9563 CVSS: 6.5
CVE-2016-3976 CVSS: 7.5
CVE-2010-5326 CVSS: 10

06 de abr.
2021

Microsoft Exchange: ProxyRCE

Continuó la explotación de nuevas vulnerabilidades de Microsoft Exchange Server, investigadores de todo el mundo buscan nuevas vulnerabilidades en este sistema a través de concursos de Bug Bounty como Pwn20wn. Se prevé un escenario de múltiples nuevas vulnerabilidades para Exchange.

CVE-2021-28480 CVSS: 9.8
CVE-2021-28481 CVSS: 9.8
CVE-2021-28482 CVSS: 8.8
CVE-2021-28483 CVSS: 9

13 de abr.
2021

RockYou2021

RockYou2021, es el diccionario de contraseñas más grande de la historia, sin embargo, no se debe confundir con el leak de credenciales COMB21, de hecho, ni siquiera está en la misma categoría ya que este archivo solo cuenta con contraseñas que no están asociadas a un usuario ni correo electrónico. Recibe su nombre de un famoso diccionario de contraseñas llamado ROCKYOU, que aparece principalmente en ejercicios de ciberseguridad y desafíos de CTF en estos días, donde los expertos en ciberseguridad y los jugadores de CTF los usan para intentar forzar un inicio de sesión o descifrar una constraseña.

25 de abr.
2021

Windows RCE Wormable

Una falla que explota la pila del protocolo HTTP. Esta pila es utilizada por el servidor IIS integrado de Windows y si este servidor está habilitado. Microsoft dice que un atacante puede enviar un paquete con formato incorrecto y ejecutar código malicioso directamente en el kernel del sistema operativo.

CVE-2021-31166 CVSS: 9.8

11 de may.
2021

20 de may.
2021

PolkIt Linux

Es una vulnerabilidad de omisión de autenticación en el servicio del sistema de autenticación polkit, que se usa en la mayoría de las distribuciones de Linux, puede permitir que un atacante sin privilegios obtenga un shell raíz.

CVE-2021-3560 CVSS: 7.8

VMWare VCenter

Continúa la activa explotación de vulnerabilidades de vSphere Client (HTML5), aparece una nueva vulnerabilidad, igual de crítica que la parcheada en febrero CVE-2021-21972.

CVE-2021-21985 CVSS: 9.8

26 de may.
2021

Windows: PrintSpooler

Vulnerabilidad de elevación de privilegios de Windows Print Spooler, la explotación de esta vulnerabilidad podría dar a los atacantes remotos el control total de los sistemas vulnerables.

CVE-2021-1675 CVSS: 8.8

08 de jun.
2021

Windows: PrintNightmare

Los investigadores aclararon que el parche de Microsoft para CVE-2021-1675 del 8 de junio estaba incompleto, lo que provocó que un nuevo exploit fuese difundido como parte de la explotación de esta vulnerabilidad, fusionándose con otras vulnerabilidades de años anteriores, obligando a la compañía a lanzar un parche de emergencia para proteger nuevamente a los usuarios.

CVE-2021-34527 CVSS: 8.8

02 de jul.
2021

Microsoft Exchange: ProxyShell

Comienza una nueva ola de parches de seguridad para vulnerabilidades activamente explotadas en Microsoft Exchange, esta vez identificadas como ProxyShell. Estas, permiten la omisión de autenticación, escalada de privilegios y la ejecución de código remoto que finalizan con la carga de una webshell remota en el servidor afectado, por lo que nuevamente son identificadas como un riesgo "crítico". ¡El plan de parcheado no puede esperar!

CVE-2021-31207 CVSS: 7.2 CVE-2021-34523 CVSS: 9.8
CVE-2021-34473 CVSS: 9.8

14 de jul.
2021

Microsoft Exchange: ProxyToken

Vulnerabilidad que permite a atacantes con cuenta dentro del mismo servidor modificar la configuración de cuentas de correo de otros usuarios permitiendo desviar el destino de todos los correos hacia el atacante. ¡Basta Exchange, ya es demasiado!,¿Parcheaste tu server con el último CU (Cumulative Update)?

CVE-2021-33766 CVSS: 7.5

14 de jul.
2021

Microsoft Exchange: ProxyOracle

Aparece un nuevo conjunto de vulnerabilidades para Microsoft Exchange, un CVE de mayo y otro de junio dan la creación del conjunto ProxyOracle. ProxyOracle permite que un atacante recupere la contraseña del usuario en formato de texto plano por completo. ¿Qué ocurre con Microsoft Exchange?, claramente afectado en 2021 por ser un activo crítico de las empresas: ¡debemos mantener sus actualizaciones a la vanguardia!

CVE-2021-31195 CVSS: 8.8 CVE-2021-31196 CVSS: 7.2

14 de jul.
2021

Linux: Sequola

Vulnerabilidad en un manejo inapropiado del búffer, permite escritura fuera de los límites establecidos permitiendo a un atacante sin privilegios escalar a administrador.

CVE-2021-33909 CVSS: 7.8

20 de jul.
2021

PetitPotam

Microsoft advierte de PetitPotam, que potencialmente se puede usar para atacar controladores de dominio de Windows u otros servidores de Windows. PetitPotam es un ataque de retransmisión NTLM clásico; Microsoft informó que ha documentado previamente estos ataques junto con numerosas opciones de mitigación para proteger a los clientes.

CVE-2021-36942 CVSS: 5.3

23 de jul.
2021

Azure ChaosDB

Llegó el turno de la nube, la vulnerabilidad en CosmosDB de Azure permite a atacantes remotos acceder como administrador a bases de dato de otros usuarios, sin que este permiso se le haya otorgado.

12 de ago.
2021

30 de ago.
2021

Atlassian: Confluence Server

Un error de inyección OGNL permite que tanto usuarios autenticados como no autenticados puedan ejecutar código arbitrario en instancias de Confluence Server y DataCenter. Durante septiembre se evidenció un alto volumen de explotación de esta vulnerabilidad debido a la liberación de diversas pruebas de concepto (PoC).

CVE-2021-26084 CVSS: 9.8

Forti Leak

Se publicó en la red TOR una filtración de credencialesde usuarios de Fortinet VPN SSL de todo el mundo, recopilada explotando un Path Traversal en el portal web de SSL VPN. Lo destacable es que aún en Chile se videncian muchos dispositivos aún vulnerables a este fallo de seguridad crítico de mayo de 2019.

CVE-2018-13379 CVSS: 9.8

07 de sep.
2021

08 de sep.
2021

Microsoft Office: Zero Day MSHTML/Trident

Vulnerabilidad en el componente MSHTML de Internet Explorer que habilita la interacción con herramientas de Microsoft Office, permitiendo que un atacante remoto pueda hacer envío de documentos con código malicioso.

CVE-2021-40444 CVSS: 7.8

Atlassian: Confluence Server (Exploit)

Se publican Pruebas de Concepto y exploits para vulnerabilidad CVE-2021-26084, permitiendo un ataque de forma automatizada.

10 de sep.
2021

14 de sep.
2021

Azure OMIGOD

Conjunto de vulnerabilidades en Azure permite que atacantes remotos accedan a servidores y escalar a privilegios Root debido a la creación del agente Open Management Infrastructure (OMI), el cual es implementado automáticamente y sin notificación al administrador una vez que se habilitan ciertos servicios alojados en una máquina Linux, OMI es un proyecto OpenSource que posiblemente esté implementado en otras plataformas y también exista la vulnerabilidad en ellas producto de este fallo de seguridad.

CVE-2021-38645 CVSS: 7.8
CVE-2021-38647 CVSS: 9.8
CVE-2021-38648 CVSS: 7.8
CVE-2021-38649 CVSS: 7.8

Vulnerabilidades SAP

Nuevo conjunto de vulnerabilidades críticas para SAP.

CVE-2021-37531 CVSS: 9.9 CVE-2021-38176 CVSS: 9.9
CVE-2021-38163 CVSS: 9.9 CVE-2021-33672 CVSS: 9.6
CVE-2021-37535 CVSS: 9.8

14 de sep. 2021

VMware vCenter Server

Esta vulnerabilidad permite que un atacante con acceso a la red mediante puerto 443 en vCenter Server ejecute códigos en el servidor mediante la carga de archivos maliciosos específicamente diseñados en el servicio de análisis. Se evidenció diversos exploit públicos en fuentes abiertas que encendieron las alarmas a nivel mundial.

CVE-2021-22005 CVSS: 9.8

22 de sep. 2021

Apache HTTP Server 2.4.49

Un cambio realizado en la normalización de rutas aplicado únicamente en la versión Apache 2.4.49, supuestamente solucionado en la 2.4.50 (se evidenció nuevo fallo posteriormente), permite que un atacante remoto no autenticado mapee URL fuera del directorio raíz, permitiendo leer archivos restringidos del sistema. (PD: En Chile, más del 60% de los servidores Apache no están en su última versión, de hecho la mayoría bajo versiones deprecadas y sin soporte).

CVE-2021-41773 CVSS: 7.5

05 de oct. 2021

Apache HTTP Server 2.4.50

Se encontró que la corrección para CVE-2021-41773 en Apache HTTP Server 2.4.50 era insuficiente. Bajo ciertas condiciones, un atacante podría usar un ataque de recorrido de ruta para asignar URL a archivos fuera de los directorios configurados por directivas similares a Alias. Este problema solo afecta a Apache 2.4.49 y Apache 2.4.50 y no a versiones anteriores. Hay que actualizar a la versión 2.4.51, tercer release en menos de 1 mes.

CVE-2021-42013 CVSS: 7.4

07 de oct. 2021

Servidores de GifLab aún sin parchear

Una falla crítica de GitLab de ejecución remota de código no autenticado, reportada y corregida en abril de 2021, mantiene aún más de la mitad de sus implementaciones sin parchear haciéndolas altamente explotables.

CVE-2021-22205 CVSS: 10

03 de nov. 2021

Exploits para vulnerabilidades de Microsoft

El acostumbrado boletín de seguridad mensual de Microsoft trajo consigo la evidencia de la activa explotación de algunas vulnerabilidades: CVE-2021-42321 (Vulnerabilidad de ejecución remota de código de Microsoft Exchange Server) y CVE-2021-41379 (Vulnerabilidad de elevación de privilegios de Windows Installer), CVE-2021-42287 y CVE-2021-42278 (Vulnerabilidad de elevación de privilegios de los servicios de dominio de Active Directory)

CVE-2021-41379 CVSS: 7.8
CVE-2021-42321 CVSS: 8.8
CVE-2021-42287 CVSS: 8.8
CVE-2021-42278 CVSS: 8.8

09 de nov. 2021

0-day Palo Alto GlobalProtect App

Existe una vulnerabilidad de corrupción de memoria en el portal GlobalProtect de Palo Alto Networks y las interfaces de puerta de enlace que permite a un atacante de red no autenticado interrumpir los procesos del sistema y potencialmente ejecutar código arbitrario con privilegios de root.

CVE-2021-3064 CVSS: 9.8

10 de nov. 2021

Activa explotación de vulnerabilidades Mikrotik

De acuerdo a la investigación realizada por nuestro equipo de especialistas en ciberinteligenia, equipos Mikrotik desde la versión 3.30 hasta la versión 6.45.6 (83 versiones), serían vulnerables. En Chile, se detectaron alrededor de 1.000 equipos con versiones vulnerables.

CVE-2019-3979 CVSS: 7.5
CVE-2019-3976 CVSS: 7.5
CVE-2019-3978 CVSS: 7.5
CVE-2018-14847 CVSS: 9.1
CVE-2019-3977 CVSS: 7.5
CVE-2018-7445 CVSS: 9.8

07 de dic. 2021

Log4Shell RCE

Apache Software Foundation ha publicado soluciones para contener una vulnerabilidad de día cero explotada activamente que afecta a la biblioteca de registro de Apache Log4j, que podría utilizarse como arma para ejecutar código malicioso y permitir una toma de control completa de los sistemas vulnerables. Diferentes proveedores de seguridad han emitido avisos que anuncian el estudio de las implicancias en sus productos.

CVE-2021-44228 CVSS: 10

09 de dic. 2021

13 de dic.
2021

Log4j versiones 1.x

Falla de deserialización no confiable que afecta a la versión 1.2 de Log4j (las versiones 1.x han llegado al final de su vida útil). Para la vulnerabilidad CVE-2021-1404, no existen esfuerzos de parchado debido a que es una versión deprecada del servicio, por lo que para su remediación solo aplica actualizar a últimas versiones.

CVE-2021-45105 CVSS: 5.9

18 de dic.
2021

Log4j RCE

Los desarrolladores de Log4j lanzaron otra actualización, la versión 2.17.1, para abordar CVE-2021-44832, una vulnerabilidad de gravedad media, la cual es vulnerable a un ataque de ejecución de código remoto (RCE), en donde un atacante con permiso para modificar el archivo de configuración de registro puede construir una configuración maliciosa utilizando un Appender JDBC con una fuente de datos que hace referencia a un URI JNDI que puede ejecutar código remoto. La versión estable actualizada a febrero de 2022 es Log4j 2.17.2

Log4Shell DoS

El lunes 13 de diciembre, después de que se descubrió que la primera actualización (versión 2.15.0), estaba "incompleta en algunas configuraciones" no predeterminadas y podría permitir que un atacante ejecutase un ataque de denegación de servicios (DoS)", el proyecto Apache Logging Services lanzó una nueva versión (Log4j 2.16.0) para mitigar esta nueva vunerabilidad identificada como CVE-2021-45046.

CVE-2021-45046 CVSS: 9

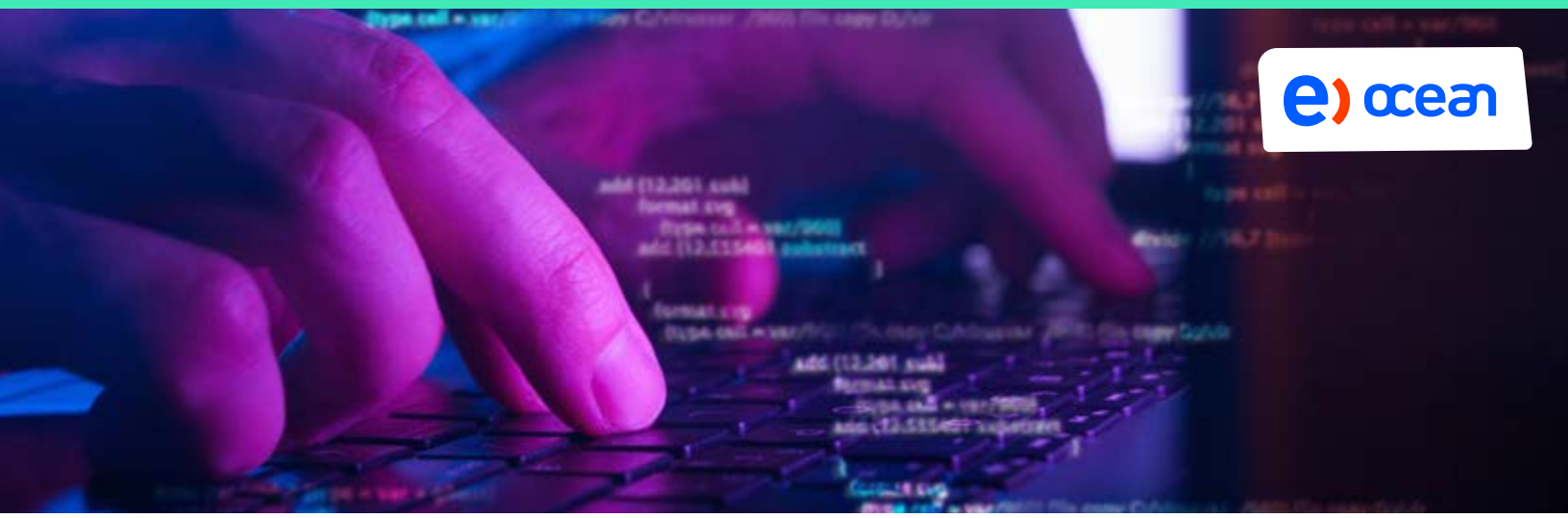
14 de dic.
2021

Log4j DoS

Vulnerabilidad de denegación de servicio que afecta a las versiones de Log4j de 2.0-beta9 a 2.16.0. Los desarrolladores de Log4j lanzaron otra actualización, la versión 2.17.0, para abordar CVE-2021-45105, una vulnerabilidad de alta gravedad que puede explotarse para ataques de denegación de servicio (DoS) mediante el envío de solicitudes especialmente diseñadas.

CVE-2021-1404 CVSS: 7.5

28 de dic.
2021



Vulnerabilidades en la infraestructura informática

La explotación de vulnerabilidades de infraestructura informática continúa siendo un vector de entrada útil para los ciber actores maliciosos. Ésto, debido a que en líneas generales, aún se presentan alguna de estas características:

- Malas políticas de parcheado
- Vulnerabilidades presentes en sistemas
- Malas prácticas de configuración
- Obsolescencia y resistencia al cambio

Durante el año 2021 se evidenció el mismo patrón respecto a años anteriores, concerniente a la resistencia al cambio y la aplicación de políticas de parcheado, las que finalmente desencadenaron un aumento de compromisos exitosos durante campañas de ataques en diferentes organizaciones.

En efecto, aún se observan sistemas obsoletos expuestos a Internet, equipos que no han sido configurados de una manera adecuada y que no han recibido un proceso de hardenización necesario para operar en ambientes donde su exposición puede significar compromiso para la red de una organización y sus enlaces con terceros.

Algunos ejemplos de este tipo son:

- Routers y dispositivos de capa 3 vulnerables y obsoletos.
- Servidores en sitios web aún sin parches a vulnerabilidades activamente explotadas.
- Sistemas operativos obsoletos sin soporte aún en producción.

Hemos evidenciado que estos fallos son provocados principalmente por un tema cultural, el cual debe ser abordado desde la premisa "dejar de pensar en implementar hoy y asegurar mañana", aplicando el concepto de **"Security by Default"** (aseguro de manera predeterminada).

Con base a lo anterior, nuestros análisis demuestran que a nivel nacional, aún se evidencian brechas de seguridad antiguas y críticas expuestas a Internet:

SMBGhost
Unpatched
CVE-2020-0796
552

HeartBleed
Unpatched
CVE-2014-0160
536

Bluekeep
Unpatched
CVE-2019-0708
216

ProxyLogon
Unpatched
(4 CVE´s)
34

EternalBlue
Unpatched
(5 CVE´s)
26

Considerando lo anterior, es primordial que las organizaciones gestionen de una manera adecuada los procesos de actualización y sanitización de estructuras de redes que son críticas y fundamentales para la operación de la organización.

Infraestructura Cloud

(Misconfiguration - S3 bucket - Virtualización)

De acuerdo a estadísticas de Gartner, los errores más comunes al momento de utilizar tecnología cloud corresponden a:

- Restricciones de acceso insuficientes (puertos de entrada y salida).
- Políticas de almacenamiento demasiado permisivas.
- Activos expuestos públicamente.
- Higiene de credenciales y su reutilización.
- Secuestro de subdominio.

Estas malas configuraciones, representan un 90% de los problemas de seguridad a los que se enfrentan las organizaciones al momento de desplegar su infraestructura en la nube.

Otro aspecto importante referente al acceso de información disponible en la nube, es la mala configuración de tecnologías de almacenamiento "Bucket", los que muchas veces se encuentran expuestos públicamente, sin un control efectivo de acceso a la información que se encuentra contenida en ellos.

De igual forma, la pandemia y la nueva modalidad de acceso a las estaciones de trabajo remotas, trajo consigo un obligado "upgrade" en los servicios virtualizados, los que pasaron de una opción poco explorada a la base del funcionamiento de la tecnología cloud y de servicios ofrecidos en ésta.

Bajo el punto anterior, los actores maliciosos idearon nuevos métodos para "responder" a esta nueva forma de operación en las organizaciones, creando malware y explotando vulnerabilidades presentes en sistemas virtualizados, que hasta hoy, permiten comprometer estructuras completas bajo el modelo de extorsión.

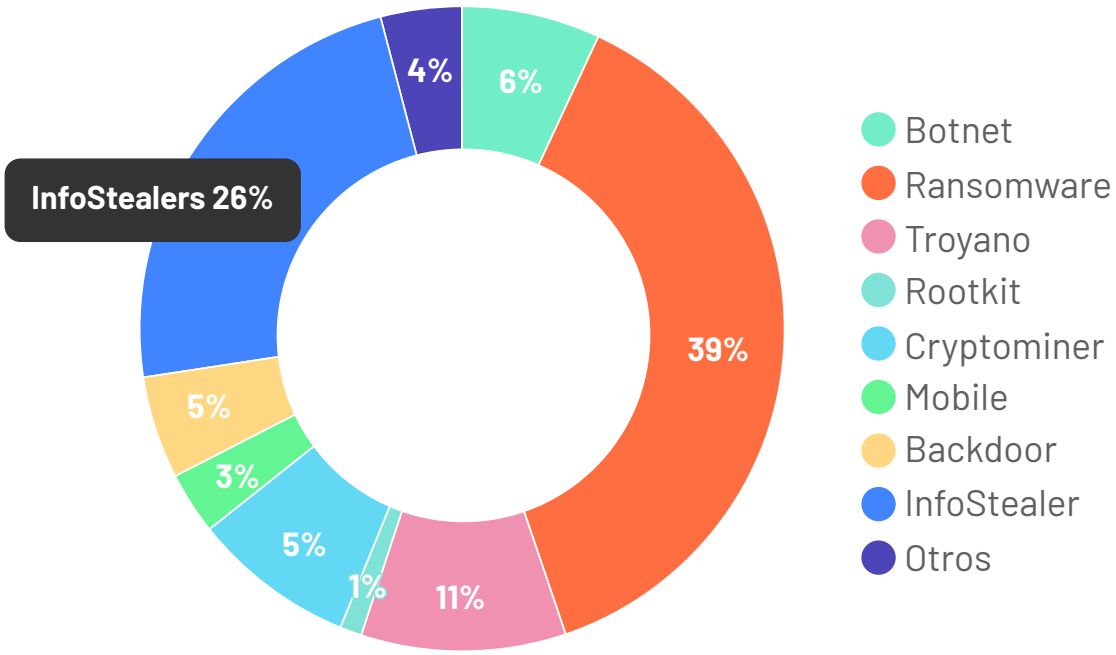
CAPÍTULO 6.
PANORAMA MALWARE EN CHILE

Por otra parte, con relación a las amenazas presentes a nivel nacional, 2021 fue un año destacado por el crecimiento de nuevas variantes de malware que marcaron una visible tendencia en cuanto a lo que hemos planteado anteriormente: **la protección de la identidad debe ser la clave de nuestras operaciones en 2022.**

La tendencia de 2021 estuvo marcada por:

- Utilización de tácticas, técnicas y procedimientos más agresivos por parte de los actores de amenaza.
- El compromiso a cadenas de suministro para comprometer objetivos de renombre mundial.
- Nuevos ataques a infraestructura crítica de naciones.
- El robo de información como principal vector de entrada para los incidentes de ciber-seguridad.
- El engaño en campañas más elaboradas contra las personas.
- La comercialización de malware como servicio (MaaS) ha conllevado un aumento sustancial en la explotación de vulnerabilidades, donde ciberdelincuentes sin mayor sofisticación ni conocimientos pueden causar un gran impacto en las organizaciones.

En efecto, de acuerdo al continuo seguimiento del panorama de amenazas que realiza nuestro equipo de especialistas de Cyber Threat Intelligence, pudimos consolidar la siguiente estadística a nivel nacional:



Si bien, ransomware es una de las amenazas más conocidas y mediáticamente más nombradas, no podemos dejar de mencionar a otro tipo de variantes de malware como Infostealers, Troyanos, Botnets y Cryptominers, cuyas cifras siguen en aumento y merecen la atención de las organizaciones nacionales y del cono Latinoamericano.

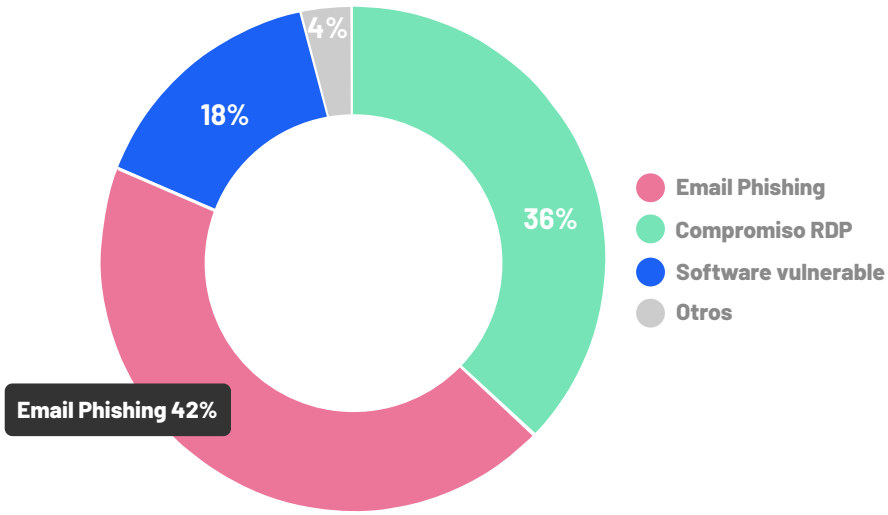
Revisa los **Indicadores de Compromiso** en nuestro GitHub

Ransomware

Tal como se mencionó en el capítulo 2 de este informe, el alza de operaciones conjuntas y combinadas contra actores de amenaza y portales de mercado negro, también estuvo presente contra grupos de ciberdelincuentes que utilizan ransomware para sus actividades ilícitas. Sin embargo, durante el año quedó demostrado que pese a los esfuerzos por desmantelar estos conglomerados delictivos, lo cierto, es que debido al ofrecimiento de servicios de alquiler de malware y la capacidad de mutación de los grupos detrás de estas operaciones maliciosas, ransomware continúa siendo una de las principales amenazas a nivel nacional y global.

Lo que marcó el año, fue la versatilidad con que algunos grupos mutaron: mientras algunos de forma voluntaria anunciaban el cese de sus operaciones, otros, se reorganizaban para cambiar sus estructuras con la intención de mantener el negocio y despistar a las autoridades encargadas de su captura, que como ya comentamos, **fue el año donde se registró el mayor número de operaciones conjuntas y combinadas contra actores de amenazas y portales de mercado negro.**

Vectores de entrada evidenciados



Evolución de ransomware

v1.0

Proliferación de ransomware por la aparición de las criptomonedas. Los respaldos diarios fueron solución de todo los problemas.

v1.5

Aparece el Ransomware-as-a-Service (RaaS), los ciber actores detrás de ransomware entienden que sus productos pueden ser comercializados en mercados negros, dando inicio a la era del comercio ransomware como servicio.

v2.0

Nace una nueva técnica, con ello los ciber delincuentes tienen mayores probabilidades de asegurar el pago de los rescates por parte de sus víctimas. La exfiltración y posterior extorsión es rápidamente adoptada por la mayoría de las nuevas variantes.

v2.5

La extorsión va más allá de las víctimas, los ciber delincuentes buscan en los datos robados, información personal de individuos que tengan relación con las víctimas (clientes, proveedores o colaboradores). En caso de encontrar algo comprometedor, envían correos electrónicos, evidenciando que han capturado datos personales por falta de seguridad de la organización comprometida. Con esto buscan asegurar aún más el pago de los rescates.

v3.0

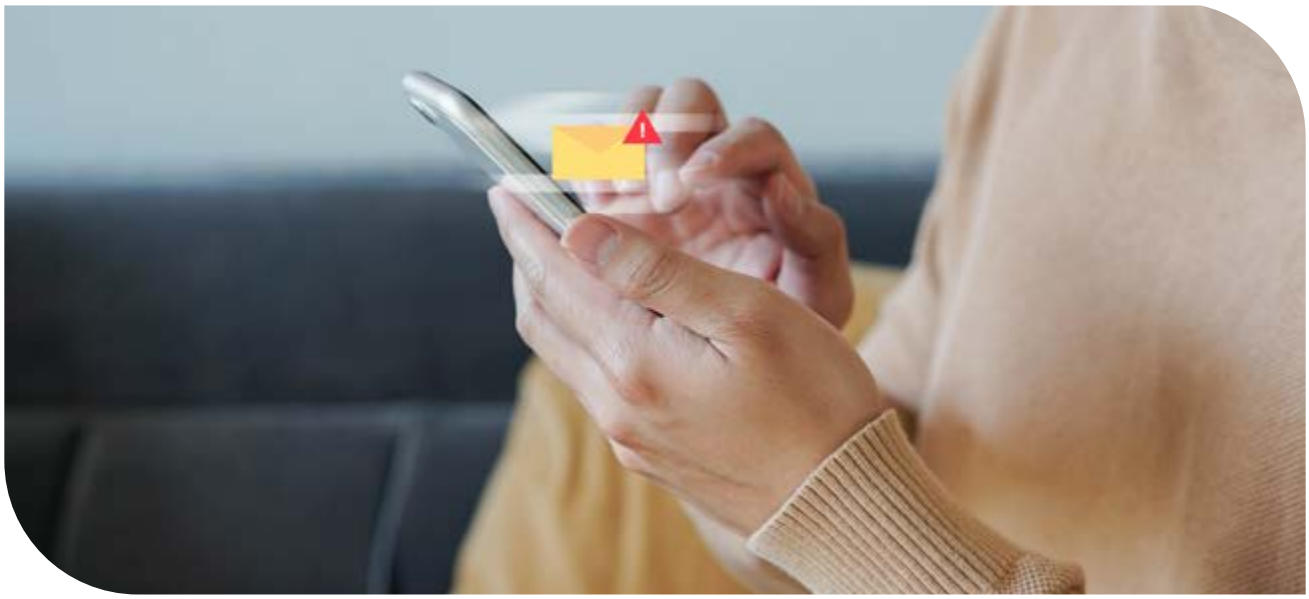
Ransomware es acompañado de una denegación de servicio distribuida (DDoS), los servicios expuestos a Internet de las víctimas no estarán disponibles hasta que se pague el rescate de los datos. Durante los últimos meses, este tipo de comportamiento se ha evidenciado de forma esporádica.

v3.5

Portales de Ransomware son privados, no hay acceso público. Durante 2021 evidenciamos grupos de ransomware como Hydra y Haron, quienes pese a ser ransomwares emergentes, se han mantenido en el anonimato debido a la dificultad que supone obtener información de ellos, ya que sus portales cuentan con una capa de autenticación que priva a equipos de seguridad su acceso rápido y por lo mismo, tienen menor impacto mediático en la comunidad.

v4.0

Ransomware se utiliza como un arma a base de código contra gobiernos e infraestructura crítica, cambiando radicalmente su motivación financiera a una motivación política-militar totalmente disruptiva. Su evolución apunta a la destrucción de sus objetivos, sin interés en beneficio económico. Hecho evidenciado en 2022 principalmente en la guerra Ruso-Ucraniana.



TOP 10 ransomware con mayor relevancia en Chile año 2021

Top	Ramson Chile 2021	Estado	Descripción
1	LockBit2.0	Online	Estado actual: online Visto por primera vez: 17/09/2020 Motivación: Beneficio económico, Disrupción Países afectados LATAM: Chile, Venezuela, Panamá, Brasil, Nicaragua, Colombia, Perú, México, Puerto Rico, Argentina.
2	Ryuk	Offline	Estado actual: offline Visto por primera vez: 13/08/2018 Motivación: Beneficio económico Países afectados LATAM: Chile, Venezuela, El Salvador, Paraguay, Perú, Panamá, Nicaragua, México, Honduras, Costa Rica, Colombia, Brasil, Bolivia, Argentina.
3	Prometheus	Offline	Estado actual: offline Visto por primera vez: 27/03/2021 Motivación: Beneficio económico Países afectados LATAM: Chile, Perú, Brasil, El Salvador, México.
4	BlackByte	Offline	Estado actual: offline Visto por primera vez: 23/08/2021 Motivación: Beneficio económico, Disrupción Países afectados LATAM: Chile, Colombia.
5	Conti	Online	Estado actual: online Visto por primera vez: 09/01/2020 Motivación: Beneficio económico, Disrupción Países afectados LATAM: Chile, México, Colombia, República Dominicana, Honduras, Nicaragua, Argentina.
6	RamsonEXX	Online	Estado actual: online Visto por primera vez: 30/11/2020 Motivación: Extorsión, Data Leak Países afectados LATAM: Chile, Ecuador, Argentina, Brasil.

Top	Ramson Chile 2021	Estado	Descripción
7	Revil/Sodinokibi	Offline	Estado actual: online Visto por primera vez: 13/05/2020 Motivación: Beneficio económico Países afectados LATAM: Chile, Perú, Brasil, México, Argentina, Trinidad y Tobago, República Dominicana.
8	Hive	Online	Estado actual: online Visto por primera vez: 23/06/2021 Motivación: Beneficio económico Países afectados LATAM: Chile, Perú, Argentina, República Dominicana, Brasil, México, Costa Rica, Colombia.
9	Spook	Offline	Estado actual: offline Visto por primera vez: 02/10/2021 Motivación: Beneficio económico Países afectados LATAM: Chile, Brasil, Paraguay, Argentina.
10	BlackMatter	Offline	Estado actual: offline Visto por primera vez: 01/08/2021 Motivación: Beneficio económico, Disrupción Países afectados LATAM: Chile, Brasil.

LockBit2.0

Es un RaaS que se encuentra en su versión de desarrollo número 2 desde junio de 2021 que cuenta con mayores y mejores capacidades auto adjudicándose como el ransomware con la mayor velocidad de cifrado de archivos.

La primera variante fue vista por primera vez en septiembre de 2019 y desde entonces ha presentando una continua actividad hasta la fecha, siendo el segundo grupo de ransomware con mayor cantidad de víctimas históricas.

- Estado actual: online
- Visto por primera vez: 17/09/2020
- Países afectados LATAM: Chile, Venezuela, Panamá, Brasil, Nicaragua, Colombia, Perú, México, Puerto Rico, Argentina.
- Motivación: Beneficio económico, disrupción.
- Modo de operación: Extorsión, data leak.

Ryuk

Ryuk es un ransomware que se identificó el 13 de agosto de 2018 el cual se propaga por vulnerabilidades en el protocolo RDP, sin embargo se han evidenciado campañas que lo distribuyen a través de malspam con archivos .PDF y .DOC habilitados con macros.

Lo que diferencia a Ryuk del resto de ransomwares no es su destreza técnica de propagación ni cifrado, sino más bien el enorme rescate que exige. La cantidad depende del tamaño de la organización afectada, sin embargo, se estima que es diez veces más que la cantidad que normalmente demandan otros malware de ese tipo.

- Estado actual: offline
- Visto por primera vez: 13/08/2018

Prometheus

Prometheus tuvo sus primeras apariciones en marzo de 2021 con gran actividad principalmente en América pero también con casos reportados desde Europa y Asia en diferentes sectores industriales, que a diferencia de otros actores, no han declarado una lista blanca o intereses específicos sobre sus ataques. En un comienzo se autodenominaba como partners de REvil, sin embargo, resultó ser parte de su estrategia para generar mayor presión en su extorsión y desvincularse su nexo con Thanos. Según diversas fuentes sus rescates oscilan entre $6.000 y $100.000 USD.

- Estado actual: offline
- Visto por primera vez: 27/03/2021
- Países afectados LATAM: Chile, Perú, Brasil, El Salvador, México.
- Motivación: Beneficio económico.
- Modo de operación: Extorsión, data leak.

BlackByte

BlackByte es un grupo de ransomware cuyas primeras publicaciones en el sitio de extorsión del grupo datan del mes de septiembre de 2021. Como parte de su funcionalidad modifica los nombres originales de los archivos bloqueados agregando '. blackbyte' como una nueva extensión.
Entre los principales sectores industriales afectados se encuentran grandes organizaciones principalmente relacionadas a infraestructura crítica desde donde es posible extorsionar y obtener cuantiosas recompensas, privilegiando calidad que cantidad.

- Estado actual: offline
- Visto por primera vez: 23/08/2021
- Países afectados LATAM: Chile, Colombia
- Motivación: Beneficio económico, disrupción.
- Modo de operación: Extorsión, data leak.

›Conti

Es un RaaS de origen Ruso con inicio de operaciones en julio de 2020 y registra la mayor cantidad de víctimas históricas de ransomwares superando por aproximadamente con creces a su par más cercano.
Pese a que durante el conflicto Rusia - Ucrania sufrió dos DataLeak importantes, este grupo aún permanece vigente y activo con constantes actualizaciones en su portal.

- Estado actual: online
- Visto por primera vez: 09/01/2020
- Países afectados LATAM: Chile, México, Colombia, República Dominicana, Honduras, Nicaragua, Argentina.
- Motivación: Beneficio económico, disrupción
- Modo de operación: extorsión, data leak.

RansomEXX

Agrupación con origen en agosto de 2020, realiza principalmente ataques de ransomware a entidades de gobierno o de infraestructura crítica y que sumando entre sus víctimas se evidencian 5 casos en LATAM georeferenciados en Chile, Argentina, Ecuador, Brasil

- Estado actual: Online
- Visto por primera vez: 30/11/2020
- Países afectados LATAM: Chile, Ecuador, Argentina y Brasil
- Motivación: Beneficio económico, disrupción.
- Modo de operación: Extorsión, data leak.

Hive

Hive Ransomware es un malware de doble extorsión que comenzó a operar en junio de 2021 utilizando todas las herramientas de extorsión disponibles para crear presión sobre la víctima, incluida la fecha del compromiso inicial, la cuenta regresiva, la fecha en que la filtración se reveló en su sitio e incluso la opción de compartir la filtración en las redes sociales.

A partir de julio de 2021, el grupo toma fuerza al reclutar nuevos clientes al programa de RaaS (Ransomware as a Service), exponiendo que sus operaciones tendrían un resultado similar a otros conocidos grupos "top" del momento.

- Estado actual: Online
- Visto por primera vez: 26/06/2021
- Países afectados LATAM: Chile, Perú, Argentina y Brasil
- Motivación: Beneficio económico.
- Modo de operación: Extorsión, data leak.

Spook

Variante de ransomware cuyas primeras publicaciones en el sitio de extorsión del grupo datan de los últimos días del mes de septiembre, siguiendo el modelo de un ransomware de doble extorsión.

Si bien este grupo generó ruido mediático, sus operaciones resultaron de corta duración lo que los llevó a sumar un total aproximado de 40 víctimas de las que no es posible evidenciar una tendencia clara hacia algún tipo de objetivos.

- Estado actual: offline
- Visto por primera vez: 02/10/2021
- Países afectados LATAM: Chile, Brasil, Paraguay, Argentina.
- Motivación: Beneficio económico.
- Modo de operación: Extorsión, data leak.

BlackMatter

Fué una variante que que había incorporado las principales fortalezas de variantes anteriores de ransomware, se incluye una variante PowerShell, toman la idea de suplantación con la capacidad de utilizar cuenta de administrador de dominio, encriptar almacenamientos compartidos y la estructura del panel de administración, toman pequeños parámetros de su código y mejoran velocidad de cifrado de 256Kb/s a 1Mb/s, su velocidad de cifrado está dada por la manipulación de solo los primeros bits de cada archivo y no su totalidad.

- Estado actual: offline
- Visto por primera vez: 01/08/2021
- Países afectados LATAM: Chile, Brasil
- Motivación: beneficio económico, disrupción.
- Modo de operación: extorsión, data leak.

Ransomware con mayor relevancia a nivel Mundial en el año 2021

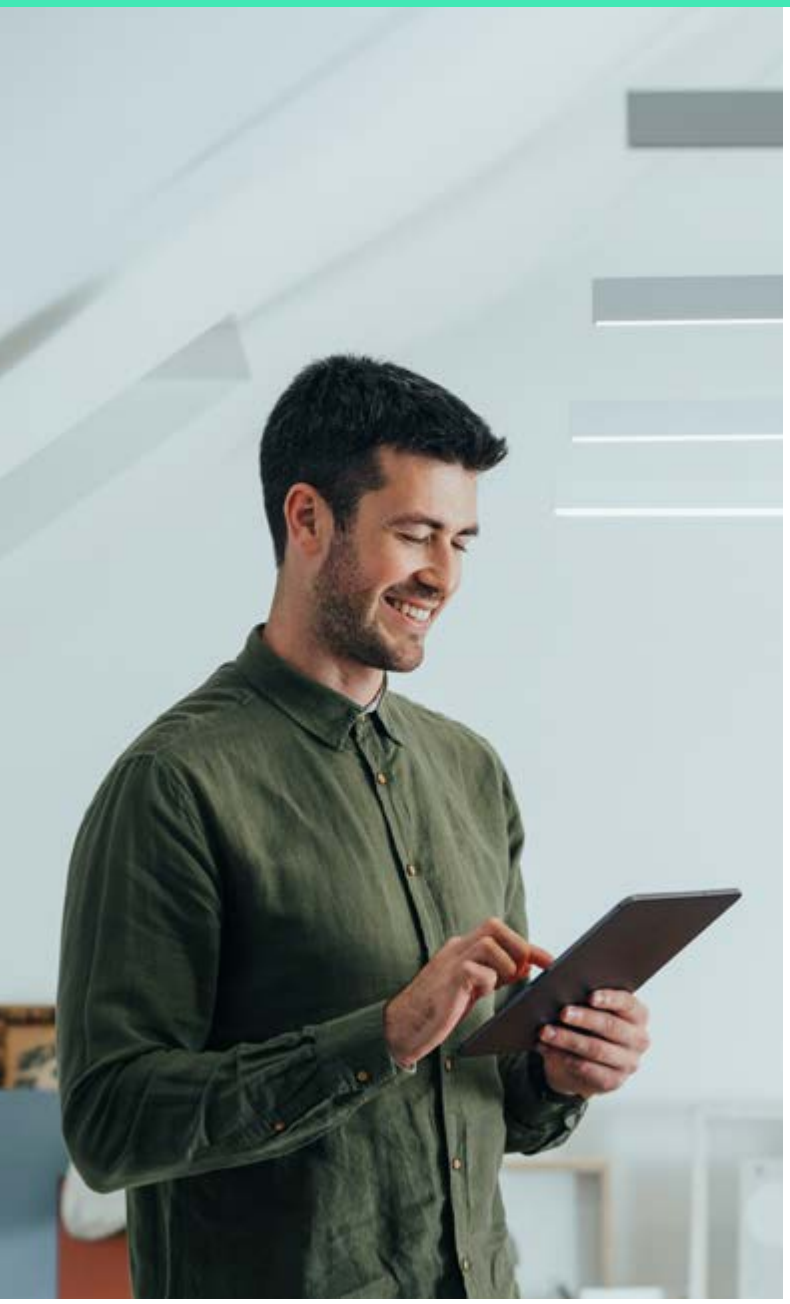
REvil/Sodinokibi

Independiente de que Ransomware REvil no tuvo presencia en Chile en el año 2021 fue uno de los grupos de ransomware más notorios o con mayor presencia mediática en el 2021.

- País origen: Atribuido a Rusia
- Estado actual: offline
- Visto por primera vez: Mayo de 2019
- Países afectados LATAM: Brasil, Perú, México y Argentina
- Motivación: Beneficio económico.
- Modo de operación: Extorsión, data leak.

Algunos hitos de este importante grupo de amenazas durante este último tiempo son los siguientes:

- El 2 de julio, la banda de ransomware REvil atacó la plataforma MSP basada en la nube de Kaseya, lo que afectó a los MSP y a sus clientes. Este ataque llamó la atención de los medios de comunicación y las autoridades policiales que aumentaron la presión sobre el grupo. A partir del 13 de julio, la infraestructura y los sitios web utilizados por la banda de ransomware REvil eran misteriosamente inalcanzables.
- El grupo regresó en septiembre de 2021 siendo evidenciado realizando ataques DDoS basados en extorsión contra ITSP en el Reino Unido y Canadá.
- En octubre de 2021 REvil anunció su cierre en una publicación que reveló que los servicios Tor de la pandilla REvil fueron presuntamente secuestrados y quien quiera que los pirateó reemplazó los servicios con una copia de las claves privadas de la pandilla, que debieron haber obtenido de una copia de seguridad anterior. Se afirmó que el servidor estaba "comprometido".



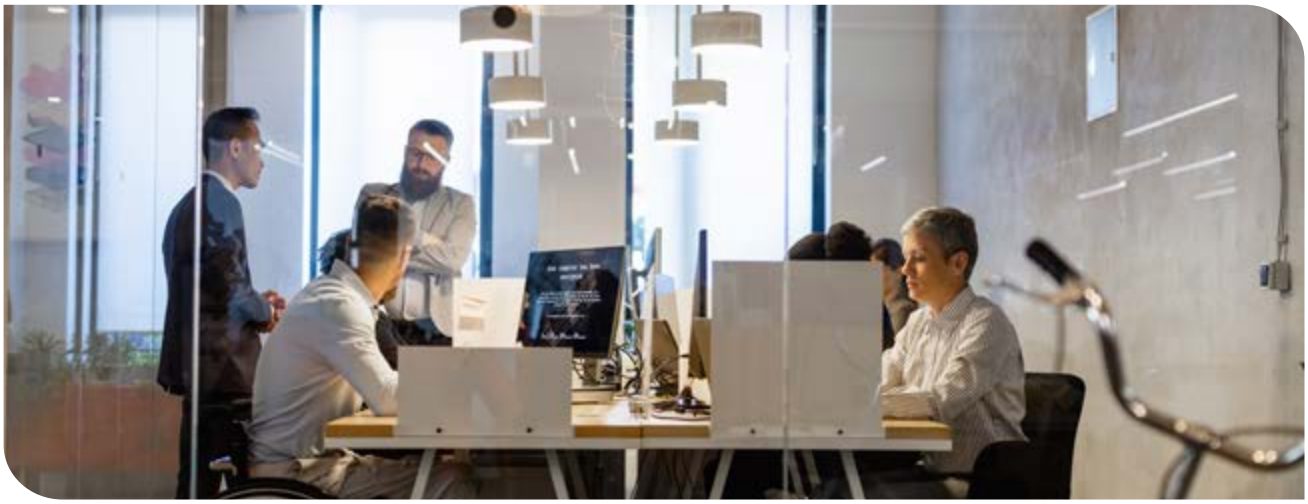
Cryptominer

XMRig, malware de criptominería que se destaca por uso de tecnología de código abierto que desafortunadamente ha venido cobrando cada vez mayor relevancia en el ambiente del malware al ser adoptada por los cibercriminales como parte de sus campañas maliciosas.

Revisa los **Indicadores de Compromiso** en nuestro GitHub

XMRig

XMRig es un software de minería de código abierto creado para facilitar el acceso a la criptominería de Monero (Criptomoneda difícil de rastrear, otorgando mayor anonimato para los ciberdelincuentes) en los equipos que se comprometen. Visto por primera vez el 26 de mayo de 2017 y con una última versión disponible de este software (6.17.0) lanzada el 17 de abril del presente año, ha sido adoptada por los cibercriminales como parte de sus campañas maliciosas para añadir funcionalidades de criptominería a su malware.



Algunos aspectos a favor de XMRig para los actores de amenazas:

- Su principal función es la distribución de trabajo a los mineros.
- Pueden modificar el código abierto según sus necesidades favoreciendo la creación de versiones troyanizadas del minero de forma activa distintas campañas.
- XMRig utiliza el protocolo de comunicación Stratum que está basado en mensajes JSON-RPC para comunicarse tanto con el servidor proxy como con el pool de minería.
- Esta comunicación suele producirse en texto claro y, por ende, es posible, en la mayoría de los casos, configurar indicadores de compromiso (IOC) en dispositivos de seguridad para detectar esta actividad en nuestra red.

› Cryptojacking como medio de infección

Los actores maliciosos detrás de campañas de malware utilizan cryptojacking para poder infectar equipos que puedan brindarles potencia informática de manera gratuita para poder minar y obtener los moneros que deseen. Esto último dado que una de las principales características por la cual eligen XMRig sobre otros mineros es que facilita su utilización en procesadores comunes por encima de las tarjetas de video (GPU), el hardware dedicado (ASIC) y el hardware programable en campo (FPGA), características que los equipos comprometidos no suelen tener.

En base a lo anterior, datos reflejan que cerca de un 73% de malware dedicados a la minería de criptomonedas utilizan a XMRig en Latinoamérica.

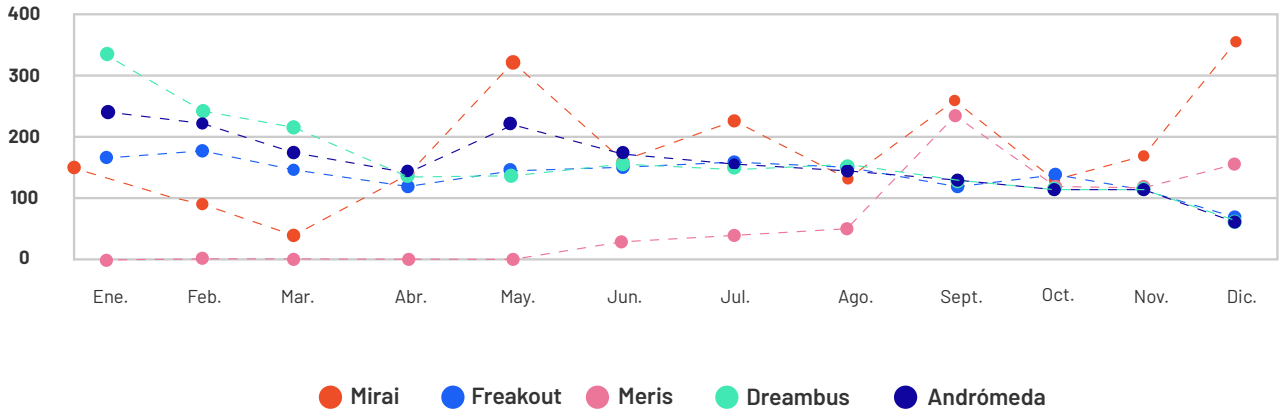
73% de malwares dedicados a la minería de criptomonedas utilizan a CMRig en Latinoamérica.

Dentro de algunas de las amenazas que utilizan a XMRig se encuentran: VictoryGate y la botnet Phorpiex, quienes se dedican a distribuir a este minero en todos equipos que infectan.

Botnet

Como se visualizó durante el año 2021, Mirai en conjunto con TrickBot siguen siendo las campañas de Botnet que registran mayor actividad en Chile.

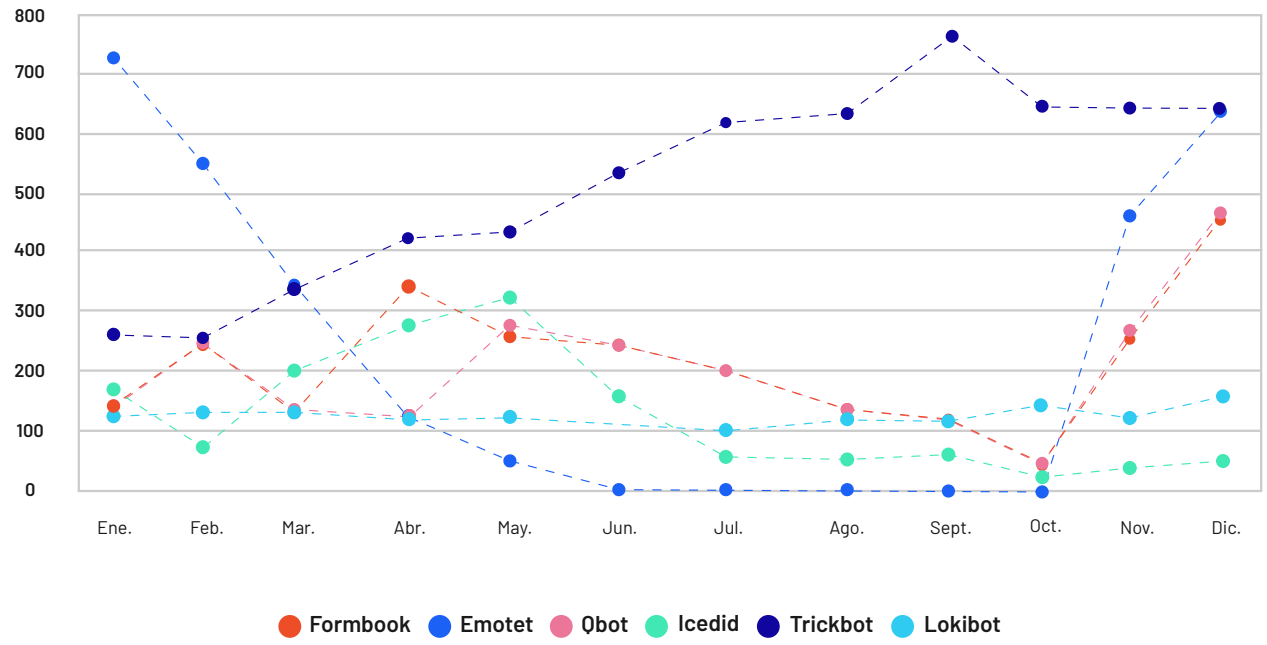
Mirai es un malware IoT de Linux que hace que las máquinas infectadas se unan a una red de botnets que se utiliza para ataques de denegación de servicio distribuido (DDoS). En el último tiempo, se ha observado una nueva variante de Mirai Linux que se propaga mediante la vulnerabilidad CVE-2021-44228 conocida como Log4Shell. Esta es posiblemente la primera variante de Mirai equipada con el código de explotación Log4Shell incorporado junto con una variante de Mirai, ya que la vulnerabilidad salió a la luz el 9 de diciembre de 2021.



Troyano bancario

En 2021, el panorama de las amenazas financieras experimentó cambios positivos al reducirse considerablemente la cifra total de usuarios afectados por malware, la cual incluye una caída del 35% en el malware para computadores personales. No obstante, las organizaciones financieras, como objetivos más lucrativos de los ciberdelincuentes, continúan enfrentando grandes cantidades de amenazas.

Según el nuevo Informe de ciberamenazas financieras en 2021 de Kaspersky, los ataques se están volviendo cada vez más corporativos en vez de estar concentrados en el consumidor. En 2021, uno de cada tres (37,8%) ataques de malware bancario para PCs eran dirigidos a usuarios corporativos, lo que representa un crecimiento de casi el 14% desde 2018.



Troyano bancarios brasileños

Al analizar estas familias, una cosa ha quedado clara: los operadores de estos troyanos bancarios parecen estar en contacto uno con el otro.

Un ejemplo es la utilización del mismo Algoritmo de cifrado personalizados en varias familias.

Otro ejemplo al examinar las cadenas de distribución (generalmente una combinación de varias etapas escritas en varios lenguajes de scripting), encontramos el uso de los mismos métodos de ofuscación o empaquetadores aplicados a diferentes guiones.

Lo nuevo este 2021

Principales familias:

- Amavaldo
- Casbaneiro
- Grandoreiro
- Guidma
- Mispadu
- Mekotio
- Zumanek
- Krachulka
- Lokorrito
- Numando
- Vadokrist
- Ousaban/Javali
- Bizarro

Grupos de actores de amenazas presentes en Chile

Una APT se refiere a una especie de ciberataque muy preciso y de alta sofisticación con múltiples vectores de ataque, ejecutado por grupos que a menudo son apoyados o financiados por entes externos, siendo su premisa:

- Acuciosidad en la seguridad de sus operaciones.
- Bajas tasas de detección.
- Altas probabilidades de éxito en el cumplimiento de sus objetivos.

Las APT que atacan a Latinoamérica, buscan la explotación de sistemas, siendo **su principal motivación la recompensa económica para financiar otras campañas manteniendo como factor indirecto, la comprobación de la efectividad de sus ataques,** entendiendo un escenario donde predominan bajos estándares de ciberseguridad presentes en las infraestructuras y menor capacidad legal para responder, respecto a otros continentes.

Durante 2021, se evidenciaron continuos ataques dirigidos contra la banca nacional, instituciones y entes gubernamentales, principalmente de grupos provenientes de China, Corea del Norte, Irán y Rusia, a continuación listamos los grupos más connotados que mantuvieron o mantienen operaciones en nuestro país:

● Aún con presencia en Chile ● Grupo desmantelado o sin campañas activas

Moses Staff

País origen: Irán
Año: 2020
Industrias afectadas:
Motivaciones:
- Espionaje
- Ventaja Militar

APT41

País origen: China
Año: 2012
Industrias afectadas:
Motivaciones:
- Espionaje
- Recompensa Económica
- Ventaja Política
- Ventaja Militar

AnonymousCL

País origen: Chile
Industrias afectadas:
Motivaciones:
- Ventaja Política
- Vandalismo
- Activismo
- EGO

KevinSecTeam

País origen: Venezuela-Colombia-Perú
Año: 2014
Industrias afectadas:
Motivaciones:
- Recompensa Económica
- Ventaja Corporativa
- Concienciación

SilverTerrier

País origen: Nigeria
Año: 2014
Industrias afectadas:
Motivaciones:
- Recompensa Económica

TA505

País origen: Rusia
Año: 2014
Industrias afectadas:
Motivaciones:
- Recompensa Económica

Hotarus Corp

País origen:
Año: 2021
Industrias afectadas:

Motivaciones:
- Recompensa Económica

FIN11

País origen: Rusia
Año: 2016
Industrias afectadas:

Motivaciones:
- Recompensa Económica

FIN9

País origen: Rusia
Año: 2015
Industrias afectadas:

Motivaciones:
- Recompensa Económica

TA551

País origen: Rusia
Año: 2018
Industrias afectadas:

Motivaciones:
- Recompensa Económica

SILENCE

País origen: Rusia
Año: 2016
Industrias afectadas:

Motivaciones:
- Recompensa Económica

APT34

País origen: Irán
Año: 2014
Industrias afectadas:

Motivaciones:
- Espionaje
- Ventaja Corporativa
- Etnicismo/Nacionalismo

APT29

País origen: Irán
Año: 2020
Industrias afectadas:

Motivaciones:
- Espionaje
- Ventaja Política
- Ventaja Militar
- Etnicismo/Nacionalismo

Lazarus Group

País origen: Corea del Norte
Año: 2009
Industrias afectadas:

Motivaciones:
- Espionaje
- Recompensa Económica
- Ventaja Política
- Ventaja Militar
- EGO
- Etnicismo/Nacionalismo

FIN4

País origen: Rumanía
Industrias afectadas:

Motivaciones:
- Espionaje
- Recompensa Económica

Sodinokibi Group

País origen:
Año: 2019
Industrias afectadas:

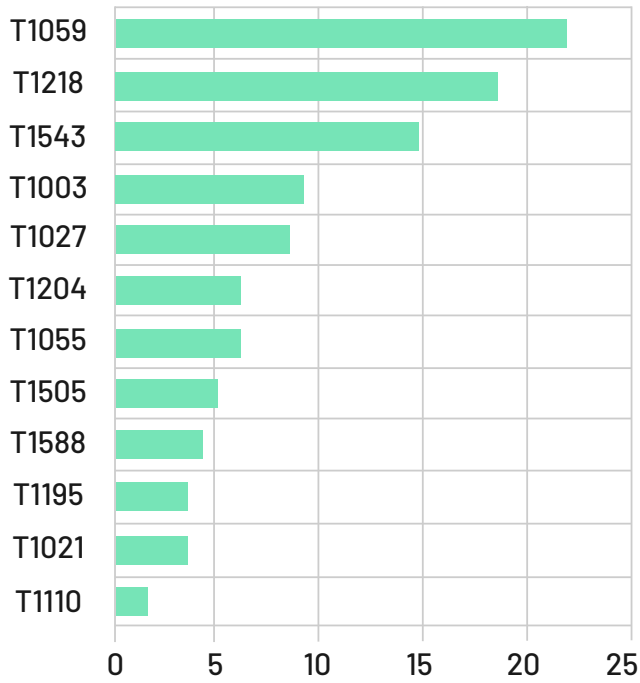
Motivaciones:
- Recompensa Económica

Trickbot Group

País origen:
Año: 2018
Industrias afectadas:

Motivaciones:
- Recompensa Económica

Técnicas **Mitre ATT&CK** más comunes



T1059

Command and Scripting Interpreter

Los ciber actores pueden abusar de los intérpretes y secuencias de comandos para ejecutar comandos, secuencias de comandos o binarios. Estas interfaces y lenguajes proporcionan formas de interactuar con los sistemas informáticos y son una característica común en muchas plataformas diferentes. La mayoría de los sistemas vienen con alguna interfaz de línea de comandos incorporada y capacidades de scripting, por ejemplo, las distribuciones de macOS y Linux incluyen algún tipo de Unix Shell, mientras que las instalaciones de Windows incluyen Windows Command Shell y PowerShell. También hay intérpretes multiplataforma como Python, así como aquellos comúnmente asociados con aplicaciones cliente como JavaScript y Visual Basic.

T1218

Signed Binary Proxy Execution

Los ciber actores pueden eludir las defensas basadas en firmas y/o procesos, mediante la ejecución de contenido maliciosos a través del la representación de autoridad de binarios firmados. Los binarios firmados con certificados digitales confiables pueden ejecutarse en sistemas Windows protegidos por validación de firma digital. Se pueden usar varios binarios firmados por Microsoft que son predeterminados en las instalaciones de Windows para ejecutar otros archivos de forma representativa por un binario autorizado.

T1543

Create or Modify System Process

Los ciber actores pueden crear o modificar procesos a nivel del sistema para ejecutar repetidamente payloads maliciosos como parte de la persistencia. Cuando los sistemas operativos se inician, pueden iniciar procesos que realizan funciones del sistema en segundo plano. En Windows y Linux, estos procesos del sistema se denominan servicios. En macOS, los procesos launchd conocidos como Launch Daemon y Launch Agent se ejecutan para finalizar la inicialización del sistema y cargar parámetros específicos del usuario.

T1003

OS Credential Dumping

Los ciber actores pueden intentar volcar las credenciales para obtener el inicio de sesión de la cuenta y el material de las credenciales, normalmente en forma de un hash o una contraseña de texto sin cifrar, desde el sistema operativo y el software. Las credenciales se pueden usar para realizar movimientos laterales y acceder a información restringida.

T1027

Obfuscated Files or Information

Los ciber actores pueden intentar hacer que un ejecutable o un archivo sea difícil de descubrir o analizar cifrando, codificando u ocultando su contenido en el sistema o en tránsito. Este es un comportamiento común que se puede utilizar en diferentes plataformas y la red para evadir las defensas.

T1204

User Execution

Los ciber actores pueden depender de acciones específicas de un usuario para lograr la ejecución de códigos maliciosos, siendo sometidos a técnicas de ingeniería social, por ejemplo, abriendo un archivo de documento malicioso o un enlace. Por lo general, estas acciones del usuario se observarán como un comportamiento de seguimiento de formas de suplantación de identidad (phishing).

T1195

Supply Chain Compromise

Los ciber actores pueden manipular productos o mecanismos de entrega de productos antes de que los reciba un consumidor final con el propósito de comprometer los datos o el sistema.

T1505 **Server Software Component**

Los ciber actores pueden abusar de las funciones legítimas de desarrollo extensible de los servidores, para establecer un acceso persistente a los sistemas. Las aplicaciones de un servidor empresarial pueden incluir características que permitan a los desarrolladores escribir e instalar software o scripts para ampliar la funcionalidad de la aplicación principal. Los adversarios pueden instalar componentes maliciosos para extender y abusar de las aplicaciones del servidor, tales como webshells, agentes o componentes en IIS.

T1588 **Obtain Capabilities**

Los ciber actores pueden comprar o robar capacidades que se pueden utilizar durante un ataque. En lugar de desarrollar sus propias capacidades internamente, los adversarios pueden comprarlas, descargarlas gratuitamente o robarlas. Las actividades pueden incluir la adquisición de malware, software (incluidas las licencias), exploits, certificados e información relacionada con vulnerabilidades.

T1021 **Remote Services**

Los ciber actores pueden usar cuentas válidas para iniciar sesión en un servicio diseñado específicamente para aceptar conexiones remotas, como telnet, SSH, SMB, RDP y VNC. El adversario puede entonces realizar acciones como el usuario que inició sesión.

T1055 **Process Injection**

Los ciber actores pueden inyectar código en los procesos para evadir las defensas basadas en procesos y posiblemente para elevar los privilegios. La inyección de proceso es un método para ejecutar código arbitrario en el espacio de un proceso activo distinto. La ejecución de código en el contexto de otro proceso puede permitir el acceso a la memoria de los procesos, los recursos del sistema o la red y posiblemente elevar privilegios. La ejecución a través de la inyección de procesos también puede eludir la detección de los sistemas de seguridad, ya que la ejecución está enmascarada bajo un proceso legítimo.

T1110

Brute Force

Los ciber actores pueden utilizar técnicas de fuerza bruta para obtener acceso a las cuentas cuando se desconocen las contraseñas o cuando se obtienen hashes de contraseñas. Sin conocer la contraseña de una cuenta o un conjunto de cuentas, un adversario puede adivinar sistemáticamente la contraseña mediante un mecanismo repetitivo o iterativo. Las contraseñas de fuerza bruta pueden tener lugar a través de la interacción con un servicio que verificará la validez de esas credenciales o fuera de línea con los datos de credenciales adquiridos previamente, como los hashes de contraseñas.

T1053

Scheduled Task/Job

Los ciber actores pueden abusar de la funcionalidad de programación de tareas para facilitar la ejecución inicial o recurrente de código malicioso. Existen utilidades dentro de los principales sistemas operativos para agendar que programas o scripts se ejecuten en una fecha y hora específicas. También se puede programar una tarea en un sistema remoto, siempre que se cumpla con la autenticación adecuada (por ejemplo, RPC y uso compartido de archivos e impresoras en entornos Windows). Programar una tarea en un sistema remoto generalmente requiere ser miembro de un administrador o de un grupo privilegiado en el sistema remoto.

T1105

Ingress Tool Transfer

Los ciber actores pueden transferir herramientas u otros archivos desde un sistema externo a un entorno comprometido. Los archivos se pueden copiar desde un sistema externo controlado por el adversario a través del canal de comando y control para llevar herramientas a la red de la víctima o mediante protocolos alternativos con otra herramienta como FTP. Los archivos también se pueden copiar en Mac y Linux con herramientas nativas como scp, rsync y sftp.

T1569

System Services

Los ciber actores pueden abusar de servicios del sistema o daemons para ejecutar comandos o programas con contenido malicioso o crear servicios de forma local o remota. Muchos servicios están configurados para ejecutarse en el arranque, lo que puede ayudar a lograr la persistencia (crear o modificar procesos del sistema), sin embargo, también se podría abusar de esta técnica para una ejecución única.

T1134

Access Token Manipulation

Los ciber actores pueden modificar tokens de acceso, para operar bajo un contexto de seguridad de sistema o usuario diferente logrando realizar acciones y evitar los controles de acceso. Windows usa tokens de acceso para determinar la propiedad de un proceso en ejecución. Un usuario puede manipular los tokens de acceso para hacer que un proceso en ejecución parezca hijo de un proceso diferente o pertenezca a otra persona que no sea el usuario que inició el proceso. Cuando esto ocurre, el proceso también toma el contexto de seguridad asociado con el nuevo token.

T1548

Abuse Elevation Control Mechanism

Los ciber actores pueden eludir los mecanismos diseñados para controlar la elevación de privilegios para obtener permisos de nivel superior. La mayoría de los sistemas modernos contienen mecanismos de control de elevación nativos destinados a limitar las acciones que un usuario puede realizar en una máquina. Se debe otorgar autorización a usuarios específicos para realizar tareas que pueden considerarse de mayor riesgo. Un adversario puede utilizar varios métodos para aprovechar los mecanismos de control integrados con el fin de escalar los privilegios en un sistema.

T1036

Masquerading

Los ciber actores pueden intentar manipular las características de sus artefactos para que parezcan legítimos o benignos para los usuarios y / o las herramientas de seguridad. El enmascaramiento ocurre cuando el nombre o la ubicación de un objeto, legítimo o malicioso, es manipulado o abusado con el fin de evadir las defensas y la observación. Esto puede incluir la manipulación de metadatos de archivos, engañar a los usuarios para que identifiquen erróneamente el tipo de archivo y dar nombres legítimos de tareas o servicios.

T1566

Phishing

Los ciber actores pueden enviar mensajes de phishing para obtener acceso a los sistemas de las víctimas. Todas las formas de suplantación de identidad (phishing) se envían electrónicamente mediante ingeniería social. El phishing puede ser dirigido, lo que se conoce como spear phishing. En el spear phishing, el adversario atacará a un individuo, empresa o industria específica.

CAPÍTULO 7.
PANORAMA PHISHING

La Ingeniería Social, es y seguirá siendo la técnica más eficiente y menos costosa para las ciberoperaciones delictuales, debido al bajo riesgo para los atacantes y su particularidad de estar orientada a la manipulación de la tendencia natural de la gente a confiar, valiéndose así de las personas y no del sistema operativo o equipamiento de seguridad.

No podemos olvidar que el usuario es el eslabón más importante de la cadena de la seguridad, por lo que su acción o inacción serán fundamentales a la hora de corregir vulnerabilidades, protegerse ante ciberataques o evitar caer en las trampas de los ciberdelincuentes.

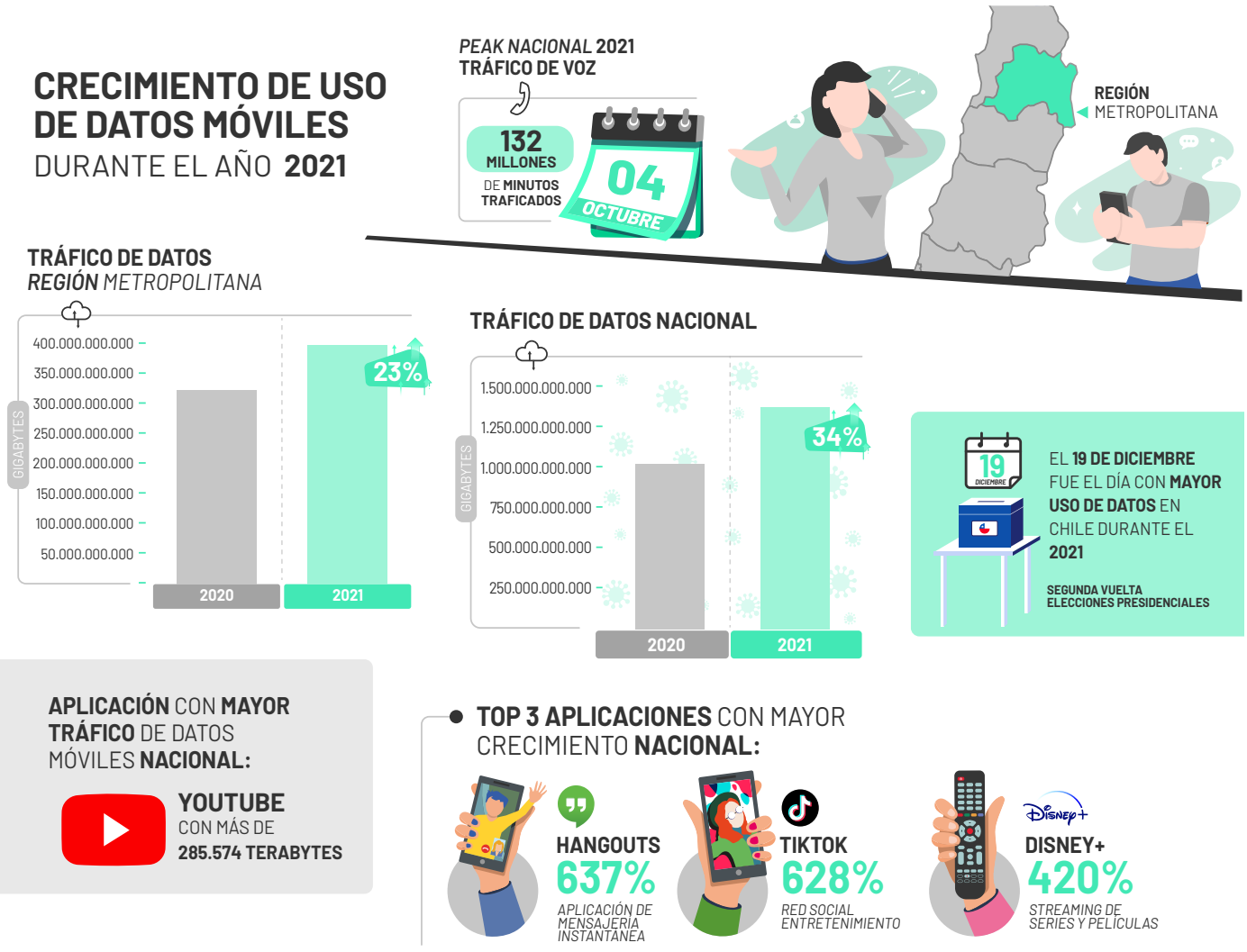
El equipo de expertos del área de Inteligencia de Entel Ocean, ha analizado algunas cifras del Panorama de Phishing 2021 a nivel nacional:

Al menos el 75% de los colaboradores de una organización, han recibido un correo phishing, de los cuales el 14% ha caído en el engaño.

Lo preocupante es el factor ponderado de criticidad, entendiendo que este tipo de acciones son en su gran mayoría el principal vector de entrada de múltiples amenazas de malware: en especial ransomware y troyanos.

Durante el año 2021, la técnica de phishing ha marcado nuevos récords como una amenaza latente que persiste tanto en las empresas como también en el ámbito personal. Esta alza se atribuye principalmente a factores asociados a la dependencia intrínseca de la humanidad hacia la tecnología. En efecto, hemos generado hábitos arraigados a la tecnología los cuales, en gran medida, son beneficiosos para la productividad, otorgando simplicidad y eficiencia en nuestra rutina. No obstante, debido a la misma digitalización de tareas e interacciones humanas, es que, muchas veces sin darnos cuenta, estamos entregando datos valiosos de nuestra vida privada y cotidianeidad: nuestra información de identificación personal (**PII**).

Bajo este mismo contexto, es importante destacar que según estadísticas de Entel S.A., a nivel nacional, durante 2021 el tráfico de datos aumentó 34% respecto a 2020, manteniendo un año más de crecimiento.



Este escenario se replica a nivel mundial, situación conocida por los cibercriminales, quienes tienen mayor información para perfilar posibles víctimas, ayudando a que sus operaciones se ejecuten de forma más robusta, dirigida y contextualizadas.

Phishing en dispositivos móviles

A nivel latinoamericano, Chile es el tercer país con más ataques de phishing hacia dispositivos móviles, donde el 36% de los usuarios asegura haber recibido un ataque de esta naturaleza.

En LATAM, Chile es el tercer país con más ataques de phishing

hacia dispositivos móviles con un

36%

Por su parte, Argentina y Panamá son los más afectados, con un 41% y 39% respectivamente. En esta lista le siguen los pasos Chile 36%, Brasil 34% y Costa Rica 32%.

Algunas de las tácticas más comunes contra dispositivos móviles son:

Vishing **Smishing** **QRishing** **Fake Apps** **Fake Chats**

Phishing en internet

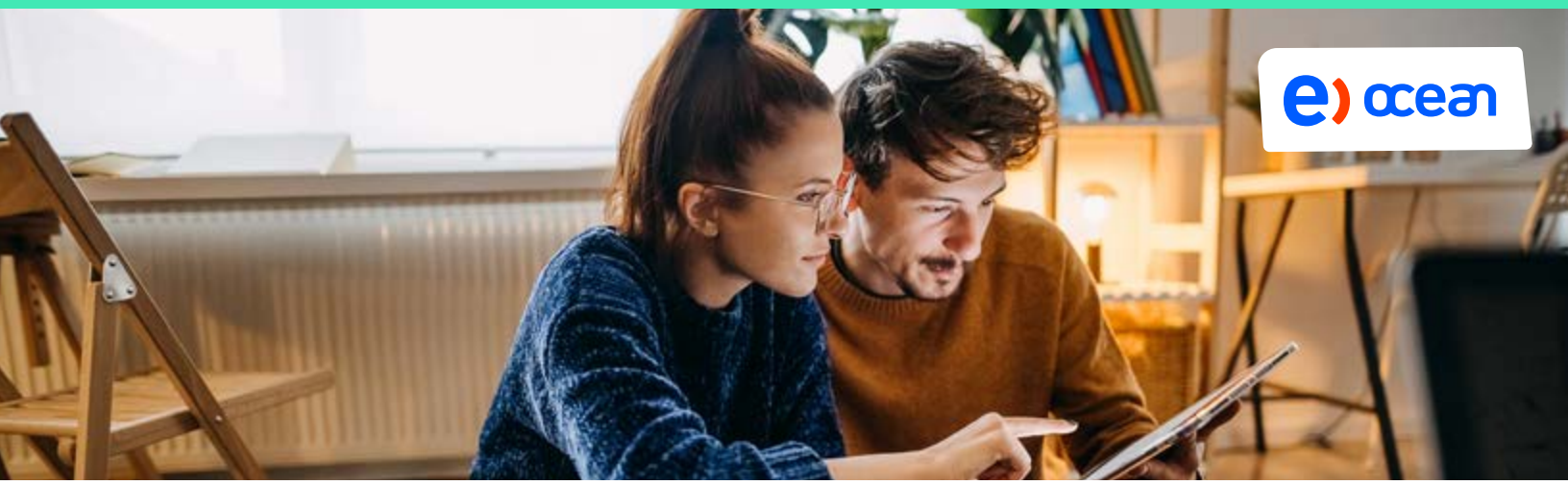
El phishing es una de las estafas más antiguas y mejor conocidas de Internet. Podemos definirlo como un tipo de fraude que emplea trucos de ingeniería social para obtener datos privados de sus víctimas o persuadirlas para que ejecuten acciones deseadas.

En este contexto, es importante destacar que gran porcentaje de las amenazas de malware son distribuidas a través de correos fraudulentos con enlaces comprometidos o archivos adjuntos maliciosos (MALSPAM).

Estos ataques pueden tener diferentes objetivos,de acuerdo a lo que se desee obtener, como por ejemplo:

- Fraude bancario a personas y empresas
- Clonación de tarjetas bancarias para su venta y/o uso en compras anónimas.
- Secuestro de credenciales empresariales para acceder a la red organizacional.
- Despliegue de malware y botnets.
- Captura de datos personales para seguimiento y/o perfilamiento de individuos.

Del mismo modo, es común observar campañas de phishing dirigidas contra organizaciones que se concentran en servidores cloud válidos y que están asociados con múltiples subdominios maliciosos. A este tipo de servidores se les conoce como “Phishing NEST” o “Nidos de Phishing”.

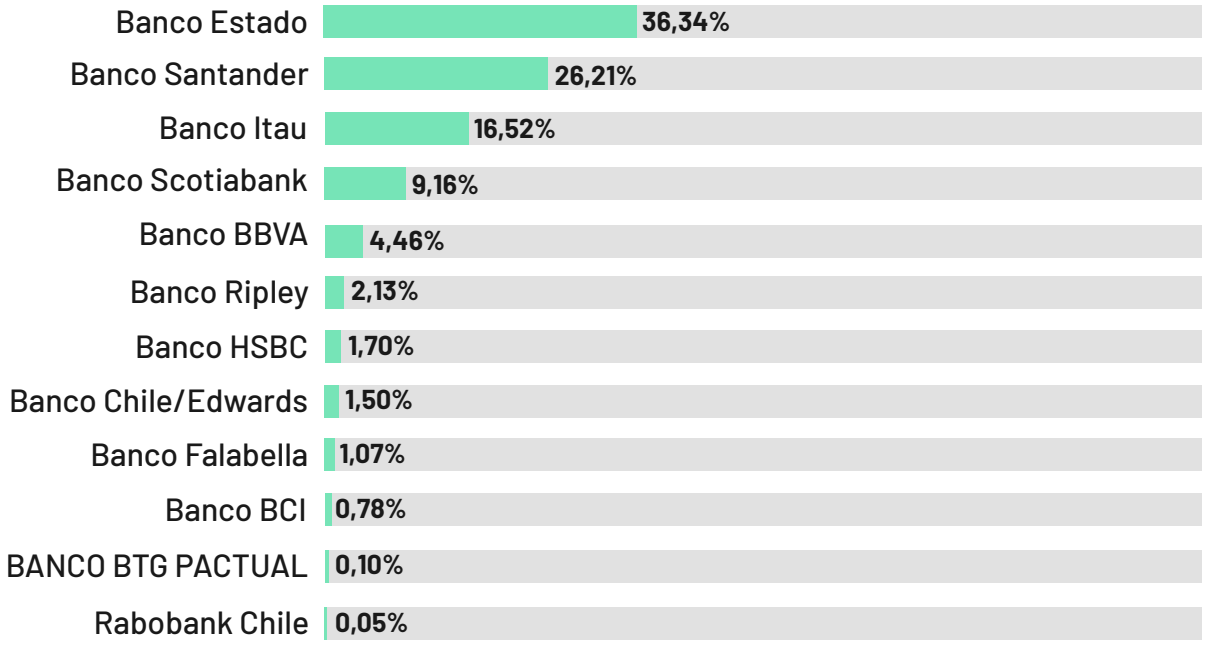


Con base en lo anterior, durante 2021 hemos destacamos a la banca como un objetivo principal para los cibercriminales, en efecto, nuestro equipo de especialistas ha llevado un seguimiento continuo de este tipo de estafas, registrando los siguientes datos a nivel nacional.

Estadísticas de bancos suplantados a nivel nacional en 2021

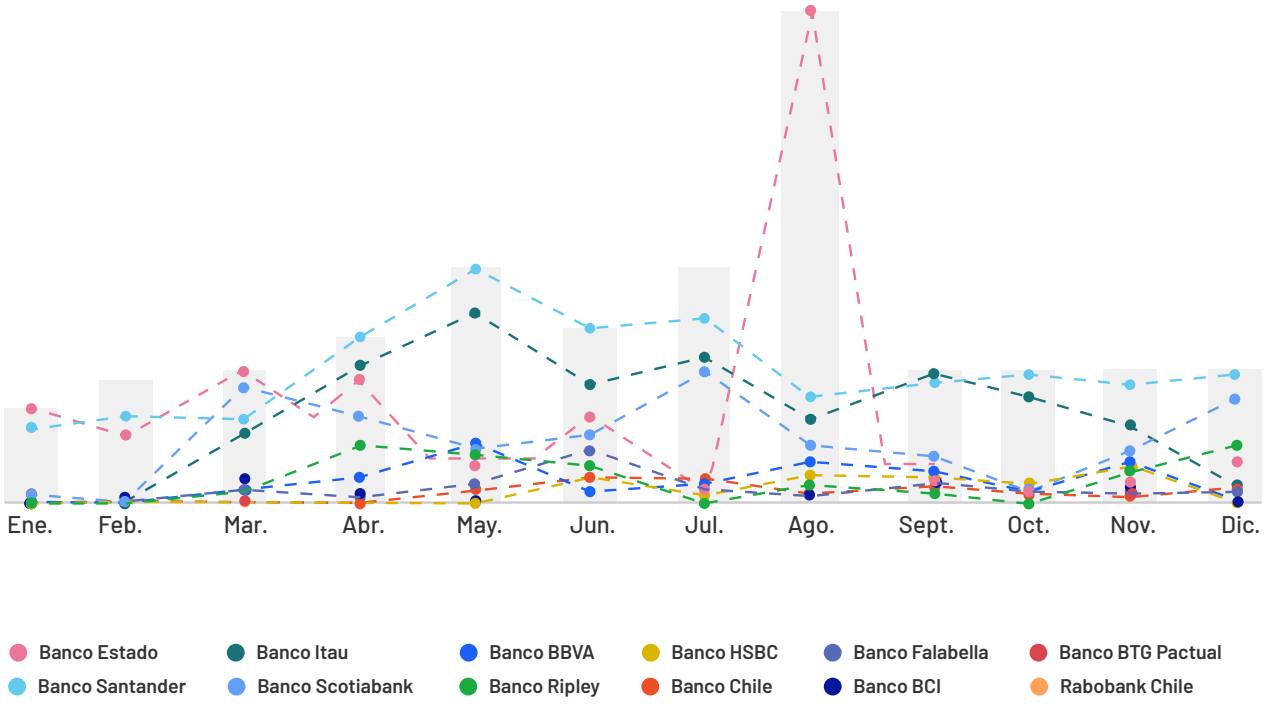
Acorde al análisis y registros de las URL que suplantan la identidad de instituciones bancarias fiscalizadas por CMF Chile, hemos podido evidenciar la siguiente tendencia en 2021:

Estadísticas de afectación a Banca nacional



Asimismo, según nuestras estadísticas, un phishing bancario en Chile tiene en promedio un ciclo de vida de aproximadamente 24 horas.

Ranking mensual de suplantaciones de bancos en Chile durante 2021



Referencias:
Bancos fiscalizados por CMF Chile - https://www.cmfchile.cl/portal/principal/613/w3-propertyvalue-29006.html

Países que dirigen ataques contra instituciones de la Banca nacional

De acuerdo con las estadísticas obtenidas por investigaciones y recolección de datos desde el área de ciberseguridad de entel, es posible detectar que las URL maliciosas mantienen orígenes desde fuera de Chile, marcando una tendencia clara los ataques provenientes desde los siguientes países:

Gráfica acumulativa 2021 - País origen de Phishing

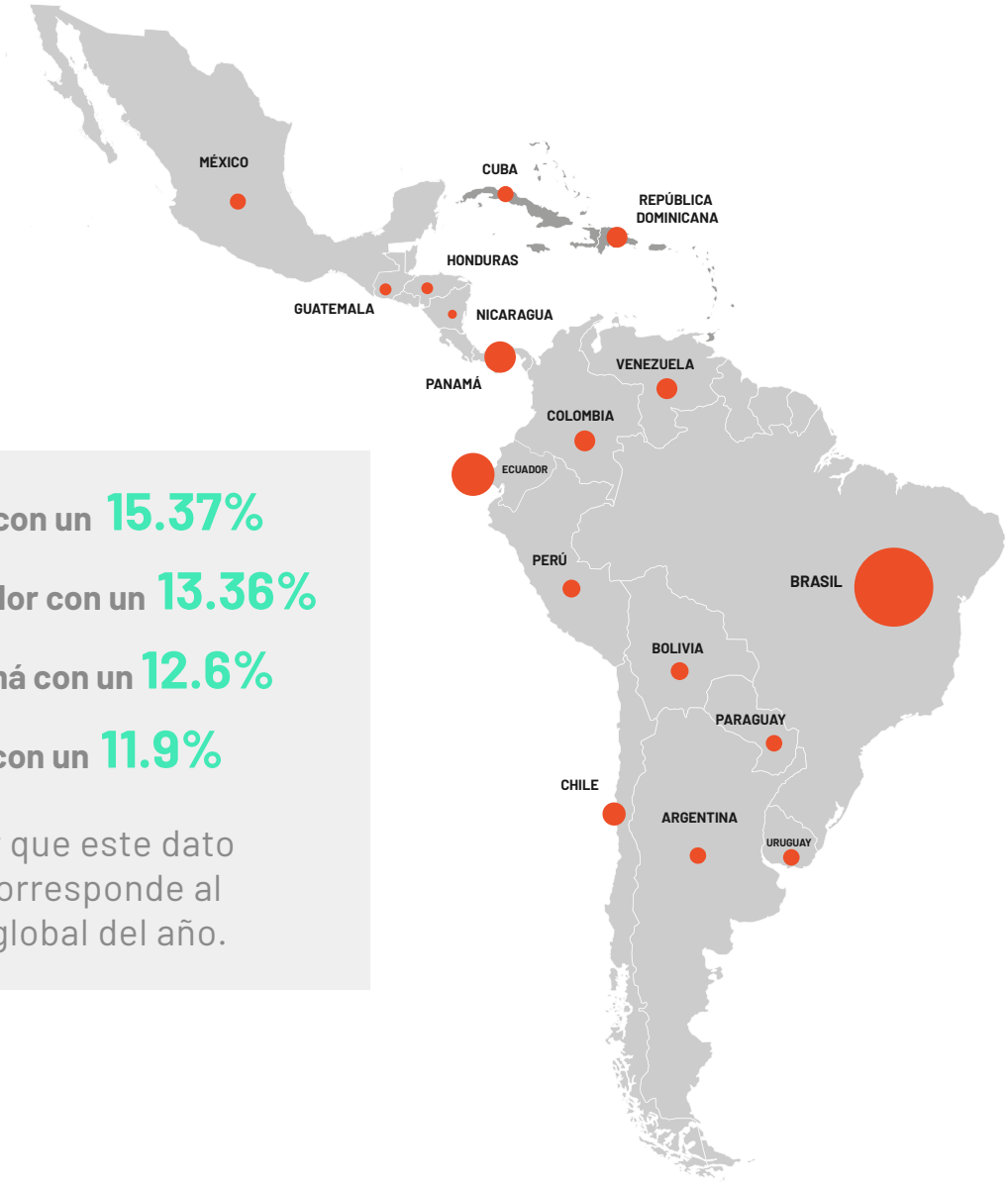
En esta distribución de ataques dirigidos a LATAM se puede evidenciar que la mayor cantidad de eventos geolocalizados por origen se distribuye de la siguiente forma:

Países de los cuales provienen los ataques	Porcentaje de origen de ataques
Estados Unidos	77,292%
Malasia	3,726%
Reino Unido	3,43%
Alemania	3,193%
Países Bajos	2,070%
Rumania	1,774%
Tailandia	1,538%
Federación de Rusia	1,538%
Canadá	1,419%
Chile	0,828%
Brasil	0,828%
Francia	0,828%
Chipre	0,769%
España	0,767%

Acorde al análisis del Phishing detectados por distintas plataformas de seguridad, en el último periodo se puede visualizar un alta tasa de ataques dirigidos a países de Latinoamérica.

Es precisamente que en este contexto que la evidencia acumulada y obtenida en el periodo nos otorga como evidencia que dentro de los mayores ataques registrados hasta el momento su distribución es:

Gráfica de Phishing a nivel latinoamericano.



1er lugar Brasil con un 15.37%

2do lugar Ecuador con un 13.36%

3er lugar Panamá con un 12.6%

4to lugar Chile con un 11.9%

Cabe destacar que este dato acumulativo corresponde al registro total global del año.

Técnicas y tendencias 2021

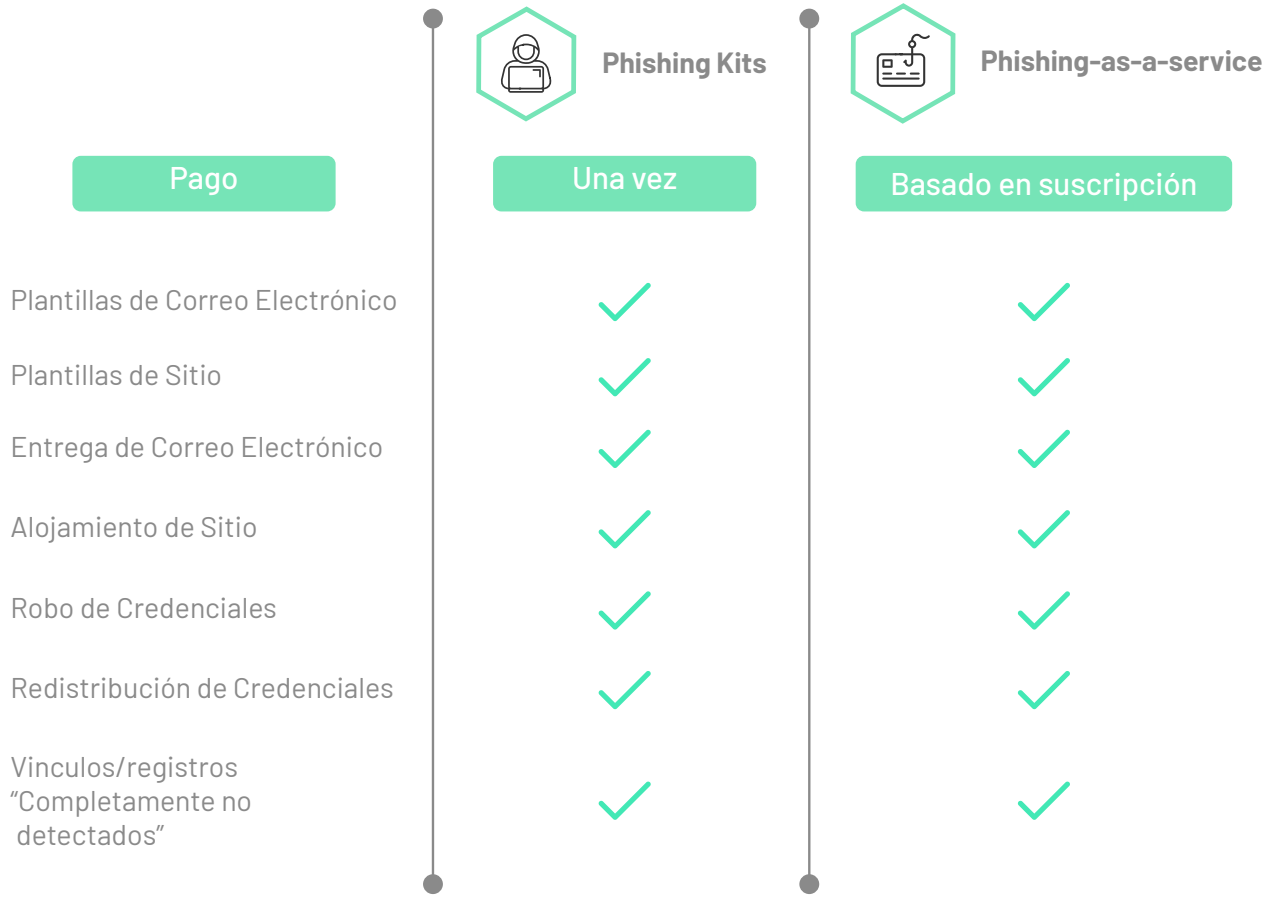
Así como muchas empresas subcontratan servicios, también lo hacen los ciberdelincuentes. En la actualidad se ha detectado el uso de kits de phishing y plantillas de correo electrónico hasta la presentación de servicios de alojamiento y automatizados con un solo pago o un modelo de negocios basado en una suscripción mensual.

1. Kits de phishing: es un conjunto de herramientas de software creadas para facilitar a personas con escasos conocimientos técnicos la creación y el lanzamiento de una campaña de phishing.

2. Phishing-as-a-service: sigue el modelo de Software-as-a-Service, que requiere que los atacantes paguen a un operador para desarrollar e implementar campañas de phishing completas a partir del desarrollo de páginas de inicio de sesión falsas, alojamiento de sitios web y análisis y redistribución de credenciales.

Como ejemplo de este tipo de campañas se grafica cómo opera el actor de amenazas BulletProofLink.

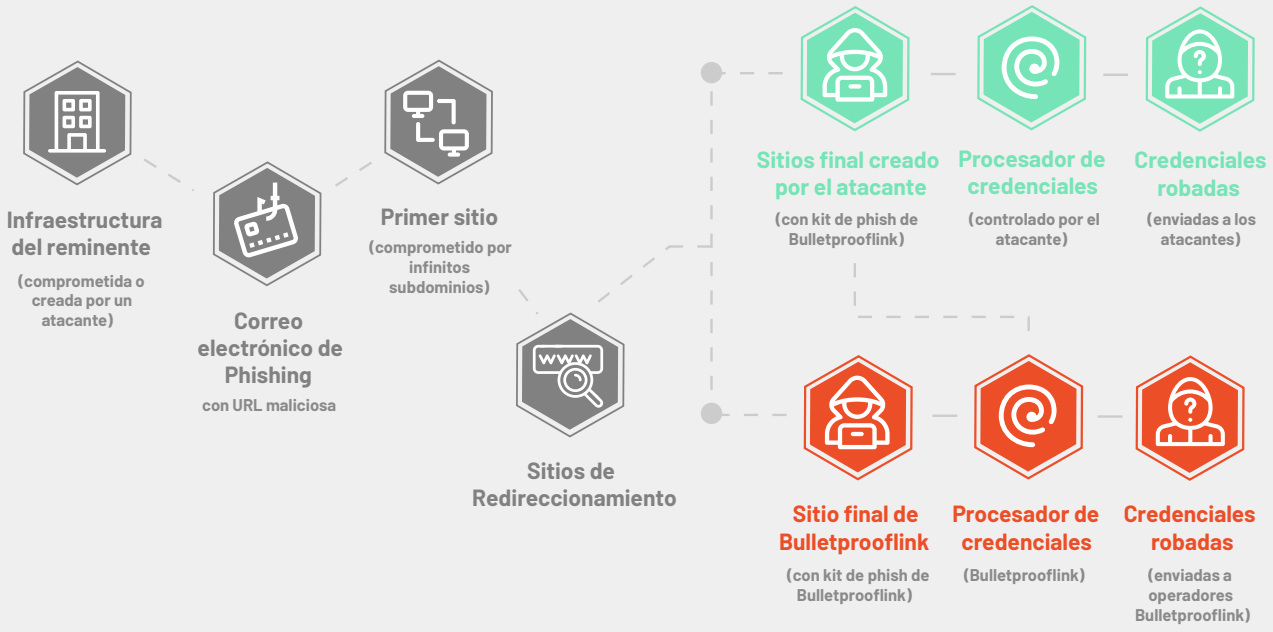
Portales globales de internet



Una de las más grandes campañas identificadas en este trimestre corresponde a Microsoft, donde el ícono de la industria declara:

"Al investigar los ataques de suplantación de identidad, nos encontramos con una campaña que utilizaba un volumen bastante alto de subdominios únicos y recién creados: más de 300.000 en una sola ejecución."

Cadena de ataques de phishing de campañas habilitadas para BulletProofLink (Microsoft)



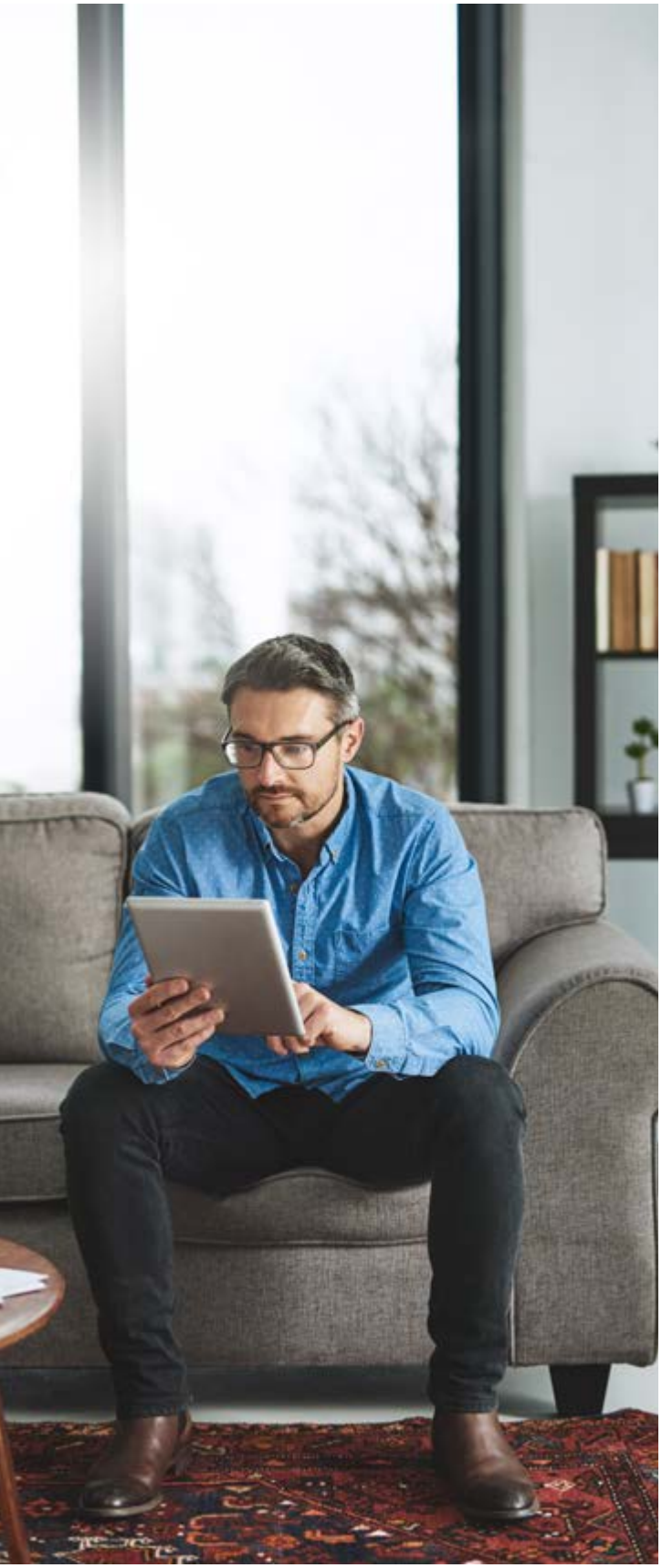
3. CAPTCHA una nueva forma de Phishing

Los ciberdelincuentes están utilizando reCAPTCHA de Google (también conocido como la función "No soy un robot") y servicios CAPTCHA para ocultar varias campañas de phishing utilizando técnicas de evasión cuyo objetivo final es escapar de la detección de los rastreadores de seguridad automatizados.

Es así que, por medio de la utilización de reCAPTCHA, logran bloquear el contenido de sus páginas de phishing y evitar que los servicios de escaneo de URL escaneen detectando el contenido malicioso, logrando finalmente otorgar un aspecto legítimo a las páginas de inicio de sesión de phishing.

Las URL maliciosas protegidas por CAPTCHA se están multiplicando

informan los investigadores de Unit 42



4. Whaling: «Pesca de ballenas», consiste en ataques de phishing dirigido contra una persona concreta de alto valor. Es igual que el phishing personalizado (Spear Phishing), pero con víctimas más exclusivas. Ni siquiera los grandes ejecutivos son inmunes a los ataques de whaling.

5. Fraude al CEO: Los phishers se hacen pasar por el director ejecutivo (CEO) o por cualquier otro alto cargo de una empresa con el fin de obtener un pago o información sobre los empleados. Las campañas de fraude de CEO son habituales tras un ataque de whaling, pues el atacante ya ha obtenido las credenciales del directivo.

6. BEC [business email compromise]: El fraude de CEO es cuando los atacantes abusan de la cuenta de correo electrónico comprometida de un CEO u otro ejecutivo de alto rango para autorizar transferencias bancarias fraudulentas a una institución financiera de su elección. Alternativamente, pueden aprovechar esa misma cuenta de correo electrónico para realizar suplantación de identidad.

› Configuraciones para tener en cuenta en tu servidor de correo

En un mundo de spam y phishing, ejecutar su propio servidor de correo electrónico está plagado de peligros. Puede ser difícil recibir sus mensajes si su servidor o dominio tiene mala reputación. No eres uno de esos servidores de correo defectuosos, pero nadie cree que tu servidor de correo sea confiable sin un montón de metadatos que lo demuestren.

En estos días, es importante conseguir las autenticaciones SPF, DKIM, DMARC y BIMI, unas herramientas que verifican la identidad de los remitentes y protegen a los destinatarios. SPF (Sender Policy Framework o Marco de Política de Remitente) crea una lista de servidores autorizados para enviar correos desde un dominio web, DKIM (DomainKeys Identified Mail o Claves de Dominio de Correo Electrónico) incluye dos cifrados para garantizar que el correo es autorizado y fiable, DMARC (Message Authentication, Reporting and Conformance o Autenticación, Informes y Cumplimiento de Mensajes) protege el dominio frente a un uso no autorizado y BIMI, o Indicadores de Marca para la Identificación de Mensajes, también tenemos registros SPF, DKIM y DMARC que ayudan a los servidores de correo a decidir si los mensajes que dicen ser de su dominio son legítimos.

Sender Policy Framework [SPF]

El Sender Policy Framework, o SPF, es una configuración de registro TXT para los DNS que brinda una capa de seguridad al encargarse de certificar qué direccionamientos pueden mandar correo en nombre de su dominio.

Este registro es eficaz contra los ataques de phishing, ya que permite a los receptores de sus correos identificar fácilmente que efectivamente provienen desde un origen legítimo y permite bloquear o marcar como ilegítimo a aquellos que no correspondan.

También ayuda a que los servidores de destino tengan más confianza y no cataloguen correos legítimos enviados por la organización como SPAM.
El hecho de tener configurado este registro sirve para que un actor malicioso no utilice nuestro dominio para enviar correos (utilizando técnicas como spoofing), ya que el receptor de dicho correo podrá validar en nuestros registros SPF si la IP/dominio desde donde se está enviado el correo con spoofing está autorizado a ser representado por nosotros.

Imortante recomendación es que exijan a sus proveedores que utilicen el mismo sistema para que nadie pueda suplantar la identidad de ellos si es que se utiliza Spoofing. Por otra parte, si la técnica utilizada es bandjacking (typosquatting), esto no tendrá efecto ya que el dominio sería otro.

DomainKeys Identified Mail [DKIM]

El DomainKeys Identified Mail, o DKIM, es un registro que permite firmar el correo con un dominio mediante claves públicas indicadas en las zonas de dominio de su organización. De este modo, el destinatario está seguro de que el correo ha sido enviado desde un servidor legítimo y no ha sido interceptado y/o reenviado desde otro servidor no autorizado.

Para este proceso son utilizadas llaves de cifrado públicas y privadas, por lo cual el emisor cifra el mensaje con su clave privada y el destinatario recibe el mensaje junto con una clave pública única que permite la visualización del mensaje.

En el caso de intentos de spoofing, la clave pública de la organización no permitirá que el mensaje desde un tercero con clave privada diferente sea considerado válido ni representativo.

BIMI

BIMI, o Indicadores de Marca para la Identificación de Mensajes, es un nuevo estándar creado para facilitar que su logotipo aparezca junto a su mensaje en la bandeja de entrada. Esto no sólo ayuda a su visibilidad, sino que BIMI está diseñado para prevenir los correos electrónicos fraudulentos y ayudar a la entrega segura (capacidad de que los emails enviados lleguen a las bandejas de entrada de los receptores asignados).

DMARC

El Domain-based Message Authentication, Reporting and Conformance, o DMARC, complementa al SPF y DKIM.

Este registro indica qué hacer cuando dan error los registros anteriores, para así poder tomar las medidas necesarias lo antes posible. Se crea un registro TXT desde el apartado de zonas DNS.

Consideraciones de implementación

Es importante mencionar que los módulos mencionados anteriormente no son vulnerabilidades propiamente tal, sino que corresponden a capas de seguridad adicionales a las ya existentes, por tanto, deben ser habilitadas y configuradas según corresponda. Con base a lo expuesto, cabe mencionar que la implementación de estas tecnologías a menudo requiere la ayuda del proveedor de infraestructura de una empresa y posiblemente incluso de un consultor, lo que hace que menos del 10% de las empresas de la mayoría de las industrias utilicen realmente las funciones de seguridad.

<10%

De las empresas de la mayoría de las industrias usan realmente las funciones de seguridad.

CAPÍTULO 8.
CONCLUSIONES

A continuación nuestras recomendaciones y reflexiones, acompañado de una guía de soluciones de acuerdo a las tendencias tecnológicas de seguridad y gestión de riesgos que estaremos enfrentando durante los próximos años.

Nuestras **Recomendaciones** Trends for 2022

Reflexiones

NO es ninguna novedad el crecimiento sostenido de **RANSOMWARE**, de la mano de **APT**, lo cual impacta directamente en los tiempos de recuperación de las organizaciones afectadas.

AUMENTO exponencial de datos y credencial exfiltradas debido directamente proporcional a redes **BOT** las cuales se encargar de indexar este tipo de información.

Crecimiento de **FRAUDE** en línea, debido a mayores habilidades y preparación de los cibercriminales, esto en directa relación con el aumento en los sistemas de las fintech, sistemas de pagos y transferencia móviles. (Aumento del TOP 10 OWASP Cross Site Forgery).

AMENAZAS con mayor grado de sofisticación para buscar el engaño o la falla humana, potenciado con cadenas de malware automatizados con incorporaciones de **IA**.

CyberSecurity **Trends 2022**

Hoy a nivel organizacional estamos enfrentando grandes desafíos a nivel global, los cuales son disruptivos para el ecosistema de ciberseguridad.

1. Atacantes mas sofisticados.
2. Brecha de habilidades en Ciberseguridad.
3. Privacidad y regulaciones normativas.
4. Aceleración y resiliencia digital.
5. Diversidad de Ciber-activos.

Las cuales están impulsando las principales tendencias, consolidadas en tres grandes grupos:

Seguridad Independiente de la Ubicación

Proteger la identidad y Privacidad de los Usuarios

- Servicio de privacidad y protección

Proteger las operaciones Cloud

- Servicio de visibilidad, cumplimiento y gobernanza
- Servicio de seguridad de la información
- Servicio de protección de la red
- Servicio de seguridad de la identidad

- Malla de ciberseguridad
- Seguridad basada en la identidad
- Seguridad para el trabajo a distancia

Evolución de Seguridad Organizacional

Programa de gestión basado en Riesgo

- Servicio de gestión de la vulnerabilidad

Proteger las operaciones Cloud

- Servicio de Gestión de Riesgos y Cumplimiento

Investigación, Detección, Respuesta y Orquestación avanzada de Incidentes

- Servicio MDR y de automatización

- Comprensión/Conciencia de ciberseguridad en el directorio
- Consolidación de proveedores de seguridad

Evolución de Seguridad Tecnológica

Proteger los nuevos procesos de negocio

- Servicio de seguridad de la aplicación NG

Probar ciberdefensas y mejorar la madurez

- Servicio de simulación de amenazas
- Servicio DRP

Protección ante amenazas avanzadas

- Servicio de NG Security Technologies

- Mejora de la privacidad
- Simulación de Brechas y Ataques (BAS)
- Gestión de las identidades de las máquinas

La estrategia es **tan relevante como la tecnología**

Cybersecurity Mesh
Rediseñar el perímetro con una visión de malla (identidad) **SASE + Zero Trust**

- Arquitectura SASE
- ZTNA
- CASB accesos SAAS Cloud

Visibilidad Consolidada
Buscar nuevas estrategias de detección con observabilidad **extendida**

- Soluciones XDR (MDR)
- Threat Hunting

NG SOC
Descentralizar la operaciones y buscar la **Automatización**
Automatización SOAR

- **Threat Intelligence Platform/Management**

Inteligencia de Amenazas
Proyectar el estado de la Ciberseguridad, complementar con operaciones de **CiberInteligencia** de amenazas.

- Nivel Cyberexposición
- **Servicios de CiberInteligencia**
- CSPM (Postura Cloud)
- BAS

NG Seguridad para Aplicaciones
Proteger las Aplicaciones desde **múltiples** dimensiones, desde su proceso de desarrollo, tiempo de ejecución y publicación

- WAAP+DDoS
- WSCC
- **RASP**

Gestión de Identidades
Gestión universal de usuarios privilegiados **Multiplataforma**.

- Sistema de control de usuarios privilegiados
- **PAM**

Es importante que comencemos a rediseñar la forma de abordar la ciberseguridad, los enfoques existentes para las arquitecturas de identidad y seguridad no son suficientes para lograr satisfacer las demandas que se modifican aceleradamente en la actualidad, principalmente impulsadas por la expansión de la superficie de ataque.

Gartner en su reciente reporte de tendencias de seguridad y gestión de riesgos considera que CyberSecurity Mesh es una de las principales y más relevantes tendencias tecnológicas, la cual a grandes rasgos considera:

- Inteligenica y analiticas de Seguridad.
- Seguridad para la identidad distribuida.
- Gestión consolidada de políticas y posturas.
- Panales consolidados e integrados.

La tendencia CyberSecurity Mesh nos propone rediseñar el perímetro con una visión de malla de ciberseguridad basada principalmente en la identidad, combinando tendencias de años anteriores que efectivamente nos ayudaron por separado a resolver problemáticas de accesos y confianza, SASE & Zero Trust respectivamente, que ahora nos invita a integrar y consolidar bajo una arquitectura de malla de ciberseguridad (CSMA).

Perimetro Cloud

La pandemia distribuyó a los equipos de trabajo de las organizaciones fuera de las oficinas comerciales y desarmó con eso uno de los más antiguos controles de seguridad: el de las defensas perimetrales. Sin este control, la navegación de los usuarios a través de Internet se ha convertido en una actividad mucho más riesgosa, donde aumenta la probabilidad de navegar en un sitio malicioso o en aquellos que fueron atacados y contaminados.

Si bien el perímetro tradicional ha sido sostenidamente sobrepasado por ataques de phishing, ataques a la cadena de suministro y otros, su utilidad para detener una amenaza, y contribuir a la detección de ataques más sofisticados, sigue vigente. Esto obliga a recomponer la estructura de controles de seguridad perimerales de una organización que difícilmente, volverán a ser como antes de la pandemia.

La respuesta de la industria ha situado el nuevo perímetro de la organización en la nube. Las tecnologías SASE, (Secure Access Service Edge) proveen una capa de variados controles de seguridad en la nube, desde la cual los usuarios navegan no sólo a los recursos de la red interna, también, a las nubes públicas dónde la organización tenga recursos o a la misma Internet. Las soluciones SASE han incorporado en esta capa, controles de acceso, detección de tráfico anómalo, identificación de malware, análisis de reputación de sitios, cifrado, detección de fuga de información, control de acceso a las nubes públicas y aislación del browser entre otros, expanden las capacidades de la organización generando nuevos casos de uso, como la navegación protegida que permite a los usuarios tener un perímetro de seguridad local cuando viajan, trabajan desde un café como así también la integración a la red de oficinas remotas, en este punto único y escalable.

a. Implementar una arquitectura SASE que sea punto de acceso a la navegación, acceso a recursos internos y acceso a la nube pública, que cuente con capacidades de control de seguridad como URL Filtering, detección de malware, detección de tráfico anómalo entre otros.

b. Implementación de tecnologías de CASB para acceso a la nube SAAS.

Zero Trust

Es el modelo de ciberseguridad con el que la industria se ha alineado con rapidez. Zero Trust, provee una mirada dónde debemos desconfiar de los accesos aún cuando estos provengan de zonas confiables como la red interna. Zero Trust, nos pide localizar controles lo más cerca posible de los datos y activos a proteger para monitorear, controlar y validar cada acceso dentro de otras cosas. El problema del modelo Zero Trust, es lograr su implementación integral. Al ser una estrategia que considera variados elementos en todo el ambiente de una organización, implica, por un lado, la expansión de controles en mayor escala y nuevas capacidades que no necesariamente se encuentran disponibles dentro de los controles ya existentes. En estricto rigor, casi cualquier control de seguridad aporta un grano de arena al modelo Zero Trust, pero son pocos los que ayudan a implementar de manera amplia y profunda esta filosofía de protección.

Microsegmentación

Es uno de los controles que hace una diferencia profunda en una estrategia Zero Trust, pero su implementación requiere algunas capacidades que no todas las tecnologías de control de acceso proveen. Una tecnología de microsegmentación debe proveer la capacidad de identificar las interacciones entre sistemas (tráfico este-oeste).

Adicionalmente, debe proveer la capacidad de construir políticas entre sistemas individuales o grupos de sistemas. Dichas políticas, deben mantenerse, aún cuando modifiquemos la localización lógica del activo.

Finalmente, debe forzar el cumplimiento de dichas políticas. Para que la microsegmentación tenga el efecto que se busca, debe poder implementarse sin tener que hacer profundos cambios en la red de la organización y debe cubrir además los mundos del datacenter y la nube. La microsegmentación limitará, seriamente, el movimiento lateral de un atacante, su exploración, la propagación de malware y el acceso a sistemas críticos dentro de su cadena de ataque. Igualmente reducirá el abuso interno y limitará el efecto que puede tener el robo de credenciales de un usuario, contribuyendo a la implementación de la estrategia Zero Trust de manera relevante y sobre todo a disminuir el riesgo de la organización.

- Desarrollar una estrategia para adoptar el modelo Zero Trust.
- Implementar la microsegmentación a nivel de servidores en la nube y en el datacenter.
- Implementación de microsegmentación a nivel de Endpoint.

›Sobre Entel Ocean

Ciberseguridad de Entel Ocean

Somos una Unidad Especializada de Entel Ocean orientada a ofrecer a las grandes empresas Servicios y Soluciones de Ciberseguridad para la protección, gestión de riesgos, cumplimiento normativo, defensa y respuesta ante amenazas cibernéticas en un mundo digital. Pionera en Chile al crear en el 2016 el primer Centro de Ciber Inteligencia, un año antes de la publicación de la Política Nacional de Ciberseguridad (PNCS) en el 2017.

¿Quién es Entel Ocean?

Somos la unidad digital de Entel, especializados en entregar soluciones seguras, flexibles y escalables para la transformación digital de tu negocio, abordando tus desafíos tecnológicos hacia una gestión más eficiente, integrada y sustentable.

- Trabajamos con las mejores tecnologías y partners de la industria.
- Tenemos expertos en cada área que te asesorarán.
- Contamos con el respaldo de Entel.
- Trabajamos con la agilidad de una startup, pero la confianza de una empresa grande.

Sobre los Autores

El presente informe del estado de la ciberseguridad es confeccionado por la unidad especializada de ciberseguridad de Entel Ocean y su centro de ciber inteligencia (CCI)

Autores del Informe:

Cyril Delaere
Director de la unidad de Ciberseguridad

Pablo Araya
Especialista Senior
Operación Ciberinteligencia

Luis Elola
Experto en Ciberseguridad

Equipo Ciber Inteligencia:

Eduardo Bouillet Carroza
Director del Centro
de Ciberinteligencia

Patricio Norambuena Salgado
Supervisor de Operaciones
de Ciberinteligencia

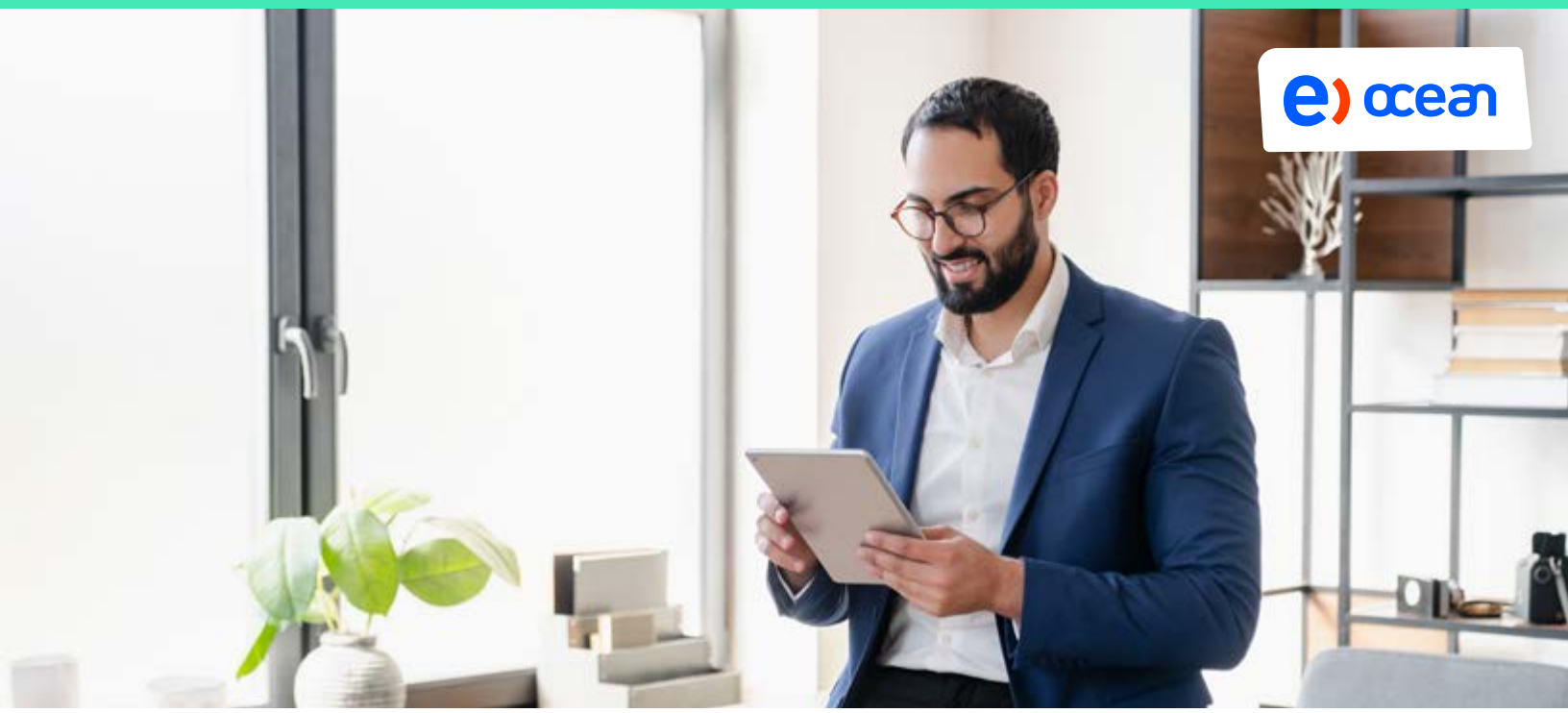
Jonathan Armijo Catalán
Analista de Ciberinteligencia

Patricio Pérez Cárcamo
Analista de Ciberinteligencia

Joaquín Miranda Gajardo
Analista de Ciberinteligencia

Inés Von Borries Reyes
Operador de Inteligencia

Jennifer Moreno Leiva
Operador de Inteligencia



Glosario

- **A.K.A:** Abreviación para la expresión Also known as, cuya traducción en español significa "también conocido como"
- **AD:** Active directory
- **API:** Interfaz de programación de aplicaciones
- **APT:** Advanced persistent threat (Amenaza persistente avanzada)
- **ASIC:** Application specific integrated circuit (Circuito integrado de aplicación específica)
- **BIMI:** Brand indicators for message identification (Indicadores de marca para la identificación de mensajes)
- **CAPTCHA:** Prueba pública de turing completamente automatizada para diferenciar a la computadora de los humanos
- **CASB:** Cloud access security broker (Agente de seguridad para el acceso a la nube)
- **CEO:** Director ejecutivo
- **CISA:** Agencia de seguridad de infraestructura y ciberseguridad
- **CSIRT:** Equipo de respuesta a incidentes de seguridad informática
- **CSMA:** Carrier sense multiple access (Acceso múltiple con escucha de señal portadora)
- **CVE:** Common vulnerabilities and exposures (Vulnerabilidades y exposiciones comunes)
- **DDoS:** Acrónimo de denegación de servicio distribuida. Técnica que utiliza numerosos hosts para realizar el ataque.
- **DKIM:** Domainkeys identified mail (Claves de dominio de correo electrónico)
- **DMARC:** Message authentication, reporting and conformance (Autenticación, informes y cumplimiento de mensajes)
- **DNS:** Sistema de nombres de dominio

- **FPGA:** Field-programmable gate array
- **GPU:** Unidad de procesamiento gráfico
- **IA:** Inteligencia artificial
- **IAM:** Gestión de identidad y acceso
- **ICI:** Infraestructuras críticas de la información
- **ICS:** Abreviación de sistema de control industrial. Es un sistema de información utilizado para controlar procesos industriales como la fabricación, el manejo de productos, la producción y la distribución.
- **IoT:** Internet of things (Internet de las cosas)
- **IT:** Tecnología de la Información
- **ITSP:** Internet telephony service provider (Proveedor de servicios de telefonía por Internet)
- **ITU:** International telecommunication union
- **MaaS:** Malware as a service (Malware como servicio)
- **MFA:** Múltiple factor de autenticación
- **MSP:** Managed services providers (Proveedor de servicios gestionados)
- **NIST:** Instituto nacional de estándares y tecnología
- **OT:** Tecnología de las operaciones
- **OTP:** One-time password (Contraseña de un solo uso)
- **PNCS:** Política nacional de ciberseguridad
- **PWCOMB21:** PassWord compilation of many breaches of 2021
- **RaaS:** Ransomware as a service (Ransomware como servicio)
- **RAT:** Remote administration tool (Troyano de acceso remoto)
- **RDP:** Protocolo de escritorio remoto
- **SAAS:** Software-as-a-service (Software como servicio)
- **SASE:** Servicio de acceso seguro (Secure access service edge)
- **SOHO:** Acrónimo de "small office-home office" (pequeña oficina-oficina en casa). Es un término que se aplica para denominar a los aparatos destinados a un uso profesional o semiprofesional pero que, a diferencia de otros modelos, no están pensados para asumir un gran volumen de trabajo.
- **SPAM:** Correo no deseado
- **SPF:** Sender policy framework (Marco de política de remitente)
- **VoIP:** Voice over internet protocol (Protocolo de voz sobre internet)

ocean

entelocean.com /entelocean /entelocean